McDermott
Will&Emery

Boston Brussels Chicago Düsseldorf Houston London Los Angeles Miami Milan
Munich New York Orange County Paris Rome Silicon Valley Washington, D.C.

Strategic alliance with MWE China Law Offices (Shanghai)

Toby H. Kusmer, P.C.
Attorney at Law
tkusmer@mwe.com
+1 617 535 4065

December 23, 2011

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this correspondence is being electronically transmitted to the United States Patent and Trademark Office on December 23, 2011
/Jessica Brown/
Jessica Brown

Commissioner for Patents
Mail Stop PATENT APPLICATION
P.O. Box 1450
Alexandria, VA 22313-1450

Re: U.S. Continuation Patent Application
Attorney Docket No. 77580-151(VRNK-1CP3CN-FT1)
SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
Subject: Transmitting Patent Application for Track I Prioritized Examination

Dear Sir/Madam:

We enclose for filing the patent application for Track I Prioritized Examination of:

Inventors: Victor Larson (Fairfax, VA); Robert Dunham Short III (Leesburg, VA); Edmond Colby Munger (Crownsville, MD); Michael Williamson (South Riding, VA)

Assignee: VIRNETX, INC.

For: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

This patent application is a continuation of U.S. Application No. 13/049,552, filed March 16, 2011, which is a continuation of U.S. Application No. 11/840,560, filed August 17, 2007, now U.S. Patent No. 7,921,211, issued April 5, 2011, which is a continuation of U.S. Application No. 10/714,849, filed November 18, 2003, now U.S. Patent No. 7,418,504, issued August 26, 2008, which is a continuation of U.S. Application No. 09/558,210, filed April 26, 2000, now abandoned, which is a continuation-in-part of U.S. Application No. 09/504,783, filed on February 15, 2000, now U.S. Patent No. 6,502,135, issued December 31, 2002, which is a continuation-in-part of U.S. Application No. 09/429,643, filed October 29, 1999, now U.S. Patent No. 7,010,604, issued March 07, 2006, which derives from U.S. Provisional Application Nos. 60/106,261, filed October 30, 1998, and 60/137,704, filed June 7, 1999, and includes:

- Certification and Request for Prioritized Examination (Track I)
- Ninety-three (93) pages of specification, claims, and abstract;
- Forty (40) sheets of drawings (Figs. 1-37);
- Application Data Sheet (6 pages);
- Declaration and Petition from parent application no. 10/714,849, signed by the inventor (6 pages)
- Power of Attorney and Statement under 37 CFR 3.73(b) from parent application no. 11/840,560, signed by the assignee

The filing fee has been calculated as shown below:

	NO. OF CLAIMS		EXTRA CLAIMS	Large Entity RATE	AMOUNT
Total Claims	28	-20	8	$60	$480.00
Independent Claims	2	-3	0	$250	$0.00
				Multiple Dependent Claim(s)	$0.00
				Basic Filing Fee	$380.00
				Search Fee	$620.00
				Examination Fee	$250.00
				Utility Application Size Fee for 50 additional sheets that exceed 100 sheets	$310.00
				Publication Fee	$300.00
				Prioritized Examination Fee (Track I) under 37 C.F.R. 1.17(c)	$4800.00
				Processing Fee 37 C.F.R. 1.17(i)	$130.00
				Total of Above Calculations	$7270.00
				Total Fee Due	**$7270.00**

☒ Please charge my Deposit Account No. 501133 in the amount of **$7270.00**. Please reference attorney docket no. 77580-151(VRNK-1CP3CN-FT1).

☒ The Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to Deposit Account No. 501133.

☒ Any additional filing fees required under 37 CFR 1.16.

☒ The Commissioner is hereby authorized to charge payment of the following fees during the pendency of this application or credit any overpayment to Deposit Account No. 501133.

☒ Any patent application processing fees under 37 CFR 1.17.

☒ Any filing fees under 37 CFR 1.16 for presentation of extra claims.

Please return the Official Filing Receipt to the undersigned.

Respectfully submitted,
McDERMOTT WILL & EMERY LLP
CUSTOMER NUMBER 23630

/Toby H. Kusmer/
Toby H. Kusmer, P.C., Reg. No. 26,418

600 13th Street, N.W.
Washington, DC 20005-3096
Telephone: (617) 535-4000
Facsimile: (617) 535-3800
Date: December 23, 2011

Doc Code: TRACK1.REQ
Document Description: TrackOne Request

PTO/SB/424 (09-11)

CERTIFICATION AND REQUEST FOR PRIORITIZED EXAMINATION (TRACK I) (Page 1 of 1)

First Named Inventor:	LARSON, Victor	Nonprovisional Application Number (if known):	
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES		

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS PRIORITIZED EXAMINATION (TRACK I) FOR THE ABOVE-IDENTIFIED APPLICATION.

1. (a) The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a). This certification and request is being filed with the utility application via EFS-Web.

   OR

   (b) The application is an original nonprovisional plant application filed under 35 U.S.C. 111(a). This certification and request is being filed with the plant application in paper. (Note: Plant applications cannot be filed via EFS-Web.)

   Note: The following are excluded from the Track I program: design applications, provisional applications, national stage applications, PCT international applications, reissue applications, and reexamination proceedings.

2. The following fees (in amounts consistent with the current fee schedule available at http://www.uspto.gov/about/offices/cfo/finance/fees.jsp) are filed with the application: (1) basic filing fee; (2) search fee; (3) examination fee; (4) any required excess claims fees; (5) any required application size fee; (6) publication fee; (7) processing fee (Track I) set forth in 37 CFR 1.17(i); and (8) prioritized examination fee (Track I) set forth in 37 CFR 1.17(c).

3. An executed oath or declaration under 37 CFR 1.63 is filed with the application.

4. The application contains or is amended to contain no more than four independent claims and no more than thirty total claims, and no multiple dependent claims.

Signature /Toby H. Kusmer/	Date 2011-12-23
Name (Print/Typed) Toby H. Kusmer, P.C.	Practitioner Registration Number 26,418

Note: *Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required in accordance with 37 CFR 1.33 and 11.18. Please see 37 CFR 1.4(d) for the form of the signature. If necessary, submit multiple forms for more than one signature, see below*.*

☑ *Total of 1 forms are submitted.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority from and is a continuation of a co-pending U.S. Application No. 13/049,552, filed March 16, 2011, which is a continuation of U.S. Application No. 11/840,560, filed August 17, 2007, now U.S. Patent No. 7,921,211, which is a continuation of U.S. Application No. 10/714,849, filed November 18, 2003, now U.S. Patent No. 7,418,504, which is a continuation of U.S. Application No. 09/558,210, filed April 26, 2000, now abandoned, which is a continuation-in-part of U.S. Application No. 09/504,783, filed on February 15, 2000, now U.S. Patent No. 6,502,135, issued December 31, 2002, which claims priority from and is a continuation-in-part patent application of previously-filed U.S. Application No. 09/429,643, filed on October 29, 1999, now U.S. Patent No. 7,010,604, issued March 07, 2006. The subject matter of U.S. application serial number 09/429,643, which is bodily incorporated herein, derives from provisional U.S. Application Nos. 60/106,261 (filed October 30, 1998) and 60/137,704 (filed June 7, 1999). The present application is also related to U.S. application serial number 09/558,209, filed April 26, 2000, now abandoned, and which is incorporated by reference herein. Each of the above-mentioned applications is incorporated herein by reference in its entirety as though fully set forth herein.

BACKGROUND OF THE INVENTION

[0002] A tremendous variety of methods have been proposed and implemented to provide security and anonymity for communications over the Internet. The variety stems, in part, from the different needs of different Internet users. A basic heuristic framework to aid in discussing these different security techniques is illustrated in FIG. 1. Two terminals, an originating terminal 100 and a destination terminal 110 are in communication over the Internet. It is desired for the communications to be secure, that is, immune to eavesdropping. For example, terminal 100 may transmit secret information to terminal 110 over the Internet 107. Also, it may be desired to prevent an eavesdropper from discovering that terminal 100 is in communication with terminal 110. For example, if terminal 100 is a user and terminal 110 hosts a web site, terminal 100's user may not want anyone in the intervening networks to know what

web sites he is "visiting." Anonymity would thus be an issue, for example, for companies that want to keep their market research interests private and thus would prefer to prevent outsiders from knowing which websites or other Internet resources they are "visiting." These two security issues may be called data security and anonymity, respectively.

[0003] Data security is usually tackled using some form of data encryption. An encryption key 48 is known at both the originating and terminating terminals 100 and 110. The keys may be private and public at the originating and destination terminals 100 and 110, respectively or they may be symmetrical keys (the same key is used by both parties to encrypt and decrypt). Many encryption methods are known and usable in this context.

[0004] To hide traffic from a local administrator or ISP, a user can employ a local proxy server in communicating over an encrypted channel with an outside proxy such that the local administrator or ISP only sees the encrypted traffic. Proxy servers prevent destination servers from determining the identities of the originating clients. This system employs an intermediate server interposed between client and destination server. The destination server sees only the Internet Protocol (IP) address of the proxy server and not the originating client. The target server only sees the address of the outside proxy. This scheme relies on a trusted outside proxy server. Also, proxy schemes are vulnerable to traffic analysis methods of determining identities of transmitters and receivers. Another important limitation of proxy servers is that the server knows the identities of both calling and called parties. In many instances, an originating terminal, such as terminal A, would prefer to keep its identity concealed from the proxy, for example, if the proxy server is provided by an Internet service provider (ISP).

[0005] To defeat traffic analysis, a scheme called Chaum's mixes employs a proxy server that transmits and receives fixed length messages, including dummy messages. Multiple originating terminals are connected through a mix (a server) to multiple target servers. It is difficult to tell which of the originating terminals are communicating to which of the connected target servers, and the dummy messages confuse eavesdroppers' efforts to detect communicating pairs by analyzing traffic. A drawback is that there is a risk that the mix server could be compromised. One way to deal with this risk is to spread the trust among multiple mixes. If one mix is compromised, the identities of the originating and target terminals may remain concealed.

Petitioner Apple Inc. - Exhibit 1002, p. 7

This strategy requires a number of alternative mixes so that the intermediate servers interposed between the originating and target terminals are not determinable except by compromising more than one mix. The strategy wraps the message with multiple layers of encrypted addresses. The first mix in a sequence can decrypt only the outer layer of the message to reveal the next destination mix in sequence. The second mix can decrypt the message to reveal the next mix and so on. The target server receives the message and, optionally, a multi-layer encrypted payload containing return information to send data back in the same fashion. The only way to defeat such a mix scheme is to collude among mixes. If the packets are all fixed-length and intermixed with dummy packets, there is no way to do any kind of traffic analysis.

[0006] Still another anonymity technique, called 'crowds,' protects the identity of the originating terminal from the intermediate proxies by providing that originating terminals belong to groups of proxies called crowds. The crowd proxies are interposed between originating and target terminals. Each proxy through which the message is sent is randomly chosen by an upstream proxy. Each intermediate proxy can send the message either to another randomly chosen proxy in the "crowd" or to the destination. Thus, even crowd members cannot determine if a preceding proxy is the originator of the message or if it was simply passed from another proxy.

[0007] ZKS (Zero-Knowledge Systems) Anonymous IP Protocol allows users to select up to any of five different pseudonyms, while desktop software encrypts outgoing traffic and wraps it in User Datagram Protocol (UDP) packets. The first server in a 2+-hop system gets the UDP packets, strips off one layer of encryption to add another, then sends the traffic to the next server, which strips off yet another layer of encryption and adds a new one. The user is permitted to control the number of hops. At the final server, traffic is decrypted with an untraceable IP address. The technique is called onion-routing. This method can be defeated using traffic analysis. For a simple example, bursts of packets from a user during low-duty periods can reveal the identities of sender and receiver.

[0008] Firewalls attempt to protect LANs from unauthorized access and hostile exploitation or damage to computers connected to the LAN. Firewalls provide a server through which all access to the LAN must pass. Firewalls are centralized systems that require

Petitioner Apple Inc. - Exhibit 1002, p. 8

administrative overhead to maintain. They can be compromised by virtual-machine applications ("applets"). They instill a false sense of security that leads to security breaches for example by users sending sensitive information to servers outside the firewall or encouraging use of modems to sidestep the firewall security. Firewalls are not useful for distributed systems such as business travelers, extranets, small teams, etc.

SUMMARY OF THE INVENTION

[0009] A secure mechanism for communicating over the internet, including a protocol referred to as the Tunneled Agile Routing Protocol (TARP), uses a unique two-layer encryption format and special TARP routers. TARP routers are similar in function to regular IP routers. Each TARP router has one or more IP addresses and uses normal IP protocol to send IP packet messages ("packets" or "datagrams"). The IP packets exchanged between TARP terminals via TARP routers are actually encrypted packets whose true destination address is concealed except to TARP routers and servers. The normal or "clear" or "outside" IP header attached to TARP IP packets contains only the address of a next hop router or destination server. That is, instead of indicating a final destination in the destination field of the IP header, the TARP packet's IP header always points to a next-hop in a series of TARP router hops, or to the final destination. This means there is no overt indication from an intercepted TARP packet of the true destination of the TARP packet since the destination could always be next-hop TARP router as well as the final destination.

[0010] Each TARP packet's true destination is concealed behind a layer of encryption generated using a link key. The link key is the encryption key used for encrypted communication between the hops intervening between an originating TARP terminal and a destination TARP terminal. Each TARP router can remove the outer layer of encryption to reveal the destination router for each TARP packet. To identify the link key needed to decrypt the outer layer of encryption of a TARP packet, a receiving TARP or routing terminal may identify the transmitting terminal by the sender/receiver IP numbers in the cleartext IP header.

[0011] Once the outer layer of encryption is removed, the TARP router determines the final destination. Each TARP packet 140 undergoes a minimum number of hops to help foil

Petitioner Apple Inc. - Exhibit 1002, p. 9

traffic analysis. The hops may be chosen at random or by a fixed value. As a result, each TARP packet may make random trips among a number of geographically disparate routers before reaching its destination. Each trip is highly likely to be different for each packet composing a given message because each trip is independently randomly determined. This feature is called *agile routing*. The fact that different packets take different routes provides distinct advantages by making it difficult for an interloper to obtain all the packets forming an entire multi-packet message. The associated advantages have to do with the inner layer of encryption discussed below. Agile routing is combined with another feature that furthers this purpose; a feature that ensures that any message is broken into multiple packets.

[0012] The IP address of a TARP router can be changed, a feature called *IP agility*. Each TARP router, independently or under direction from another TARP terminal or router, can change its IP address. A separate, unchangeable identifier or address is also defined. This address, called the TARP address, is known only to TARP routers and terminals and may be correlated at any time by a TARP router or a TARP terminal using a Lookup Table (LUT). When a TARP router or terminal changes its IP address, it updates the other TARP routers and terminals which in turn update their respective LUTs.

[0013] The message payload is hidden behind an inner layer of encryption in the TARP packet that can only be unlocked using a session key. The session key is not available to any of the intervening TARP routers. The session key is used to decrypt the payloads of the TARP packets permitting the data stream to be reconstructed.

[0014] Communication may be made private using link and session keys, which in turn may be shared and used according to any desired method. For example, public/private keys or symmetric keys may be used.

[0015] To transmit a data stream, a TARP originating terminal constructs a series of TARP packets from a series of IP packets generated by a network (IP) layer process. (Note that the terms "network layer," "data link layer," "application layer," etc. used in this specification correspond to the Open Systems Interconnection (OSI) network terminology.) The payloads of these packets are assembled into a block and chain-block encrypted using the session key. This

assumes, of course, that all the IP packets are destined for the same TARP terminal. The block is then interleaved and the interleaved encrypted block is broken into a series of payloads, one for each TARP packet to be generated. Special TARP headers IP_T are then added to each payload using the IP headers from the data stream packets. The TARP headers can be identical to normal IP headers or customized in some way. They should contain a formula or data for deinterleaving the data at the destination TARP terminal, a time-to-live (TTL) parameter to indicate the number of hops still to be executed, a data type identifier which indicates whether the payload contains, for example, TCP or UDP data, the sender's TARP address, the destination TARP address, and an indicator as to whether the packet contains real or decoy data or a formula for filtering out decoy data if decoy data is spread in some way through the TARP payload data.

[0016] Note that although chain-block encryption is discussed here with reference to the session key, any encryption method may be used. Preferably, as in chain block encryption, a method should be used that makes unauthorized decryption difficult without an entire result of the encryption process. Thus, by separating the encrypted block among multiple packets and making it difficult for an interloper to obtain access to all of such packets, the contents of the communications are provided an extra layer of security.

[0017] Decoy or dummy data can be added to a stream to help foil traffic analysis by reducing the peak-to-average network load. It may be desirable to provide the TARP process with an ability to respond to the time of day or other criteria to generate more decoy data during low traffic periods so that communication bursts at one point in the Internet cannot be tied to communication bursts at another point to reveal the communicating endpoints.

[0018] Dummy data also helps to break the data into a larger number of inconspicuously-sized packets permitting the interleave window size to be increased while maintaining a reasonable size for each packet. (The packet size can be a single standard size or selected from a fixed range of sizes.) One primary reason for desiring for each message to be broken into multiple packets is apparent if a chain block encryption scheme is used to form the first encryption layer prior to interleaving. A single block encryption may be applied to a portion, or entirety, of a message, and that portion or entirety then interleaved into a number of separate

Petitioner Apple Inc. - Exhibit 1002, p. 11

packets. Considering the agile IP routing of the packets, and the attendant difficulty of reconstructing an entire sequence of packets to form a single block-encrypted message element, decoy packets can significantly increase the difficulty of reconstructing an entire data stream.

[0019] The above scheme may be implemented entirely by processes operating between the data link layer and the network layer of each server or terminal participating in the TARP system. Because the encryption system described above is insertable between the data link and network layers, the processes involved in supporting the encrypted communication may be completely transparent to processes at the IP (network) layer and above. The TARP processes may also be completely transparent to the data link layer processes as well. Thus, no operations at or above the Network layer, or at or below the data link layer, are affected by the insertion of the TARP stack. This provides additional security to all processes at or above the network layer, since the difficulty of unauthorized penetration of the network layer (by, for example, a hacker) is increased substantially. Even newly developed servers running at the session layer leave all processes below the session layer vulnerable to attack. Note that in this architecture, security is distributed. That is, notebook computers used by executives on the road, for example, can communicate over the Internet without any compromise in security.

[0020] IP address changes made by TARP terminals and routers can be done at regular intervals, at random intervals, or upon detection of "attacks." The variation of IP addresses hinders traffic analysis that might reveal which computers are communicating, and also provides a degree of immunity from attack. The level of immunity from attack is roughly proportional to the rate at which the IP address of the host is changing.

[0021] As mentioned, IP addresses may be changed in response to attacks. An attack may be revealed, for example, by a regular series of messages indicating that a router is being probed in some way. Upon detection of an attack, the TARP layer process may respond to this event by changing its IP address. In addition, it may create a subprocess that maintains the original IP address and continues interacting with the attacker in some manner.

[0022] Decoy packets may be generated by each TARP terminal on some basis determined by an algorithm. For example, the algorithm may be a random one which calls for the

Petitioner Apple Inc. - Exhibit 1002, p. 12

generation of a packet on a random basis when the terminal is idle. Alternatively, the algorithm may be responsive to time of day or detection of low traffic to generate more decoy packets during low traffic times. Note that packets are preferably generated in groups, rather than one by one, the groups being sized to simulate real messages. In addition, so that decoy packets may be inserted in normal TARP message streams, the background loop may have a latch that makes it more likely to insert decoy packets when a message stream is being received. Alternatively, if a large number of decoy packets is received along with regular TARP packets, the algorithm may increase the rate of dropping of decoy packets rather than forwarding them. The result of dropping and generating decoy packets in this way is to make the apparent incoming message size different from the apparent outgoing message size to help foil traffic analysis.

[0023] In various other embodiments of the invention, a scalable version of the system may be constructed in which a plurality of IP addresses are preassigned to each pair of communicating nodes in the network. Each pair of nodes agrees upon an algorithm for "hopping" between IP addresses (both sending and receiving), such that an eavesdropper sees apparently continuously random IP address pairs (source and destination) for packets transmitted between the pair. Overlapping or "reusable" IP addresses may be allocated to different users on the same subnet, since each node merely verifies that a particular packet includes a valid source/destination pair from the agreed-upon algorithm. Source/destination pairs are preferably not reused between any two nodes during any given end-to-end session, though limited IP block sizes or lengthy sessions might require it.

[0024] Further improvements described in this continuation-in-part application include: (1) a load balancer that distributes packets across different transmission paths according to transmission path quality; (2) a DNS proxy server that transparently creates a virtual private network in response to a domain name inquiry; (3) a large-to-small link bandwidth management feature that prevents denial-of service attacks at system chokepoints; (4) a traffic limiter that regulates incoming packets by limiting the rate at which a transmitter can be synchronized with a receiver; and (5) a signaling synchronizer that allows a large number of nodes to communicate with a central node by partitioning the communication function between two separate entities.

Petitioner Apple Inc. - Exhibit 1002, p. 13

[0025] The present invention provides key technologies for implementing a secure virtual Internet by using a new agile network protocol that is built on top of the existing Internet protocol (IP). The secure virtual Internet works over the existing Internet infrastructure, and interfaces with client applications the same way as the existing Internet. The key technologies provided by the present invention that support the secure virtual Internet include a "one-click" and "no-click" technique to become part of the secure virtual Internet, a secure domain name service (SDNS) for the secure virtual Internet, and a new approach for interfacing specific client applications onto the secure virtual Internet. According to the invention, the secure domain name service interfaces with existing applications, in addition to providing a way to register and serve domain names and addresses.

[0026] According to one aspect of the present invention, a user can conveniently establish a VPN using a "one-click" or a "no-click" technique without being required to enter user identification information, a password and/or an encryption key for establishing a VPN. The advantages of the present invention are provided by a method for establishing a secure communication link between a first computer and a second computer over a computer network, such as the Internet. In one embodiment, a secure communication mode is enabled at a first computer without a user entering any cryptographic information for establishing the secure communication mode of communication, preferably by merely selecting an icon displayed on the first computer. Alternatively, the secure communication mode of communication can be enabled by entering a command into the first computer. Then, a secure communication link is established between the first computer and a second computer over a computer network based on the enabled secure communication mode of communication. According to the invention, it is determined whether a secure communication software module is stored on the first computer in response to the step of enabling the secure communication mode of communication. A predetermined computer network address is then accessed for loading the secure communication software module when the software module is not stored on the first computer. Subsequently, the proxy software module is stored in the first computer. The secure communication link is a virtual private network communication link over the computer network. Preferably, the virtual private network can be based on inserting into each data packet one or more data values that vary according to a pseudo-random sequence. Alternatively, the virtual private network can be based

on a computer network address hopping regime that is used to pseudorandomly change computer network addresses or other data values in packets transmitted between the first computer and the second computer, such that the second computer compares the data values in each data packet transmitted between the first computer and the second computer to a moving window of valid values. Yet another alternative provides that the virtual private network can be based on a comparison between a discriminator field in each data packet to a table of valid discriminator fields maintained for the first computer.

[0027] According to another aspect of the invention, a command is entered to define a setup parameter associated with the secure communication link mode of communication. Consequently, the secure communication mode is automatically established when a communication link is established over the computer network.

[0028] The present invention also provides a computer system having a communication link to a computer network, and a display showing a hyperlink for establishing a virtual private network through the computer network. When the hyperlink for establishing the virtual private network is selected, a virtual private network is established over the computer network. A non-standard top-level domain name is then sent over the virtual private network communication to a predetermined computer network address, such as a computer network address for a secure domain name service (SDNS).

[0029] The present invention provides a domain name service that provides secure computer network addresses for secure, non-standard top-level domain names. The advantages of the present invention are provided by a secure domain name service for a computer network that includes a portal connected to a computer network, such as the Internet, and a domain name database connected to the computer network through the portal. According to the invention, the portal authenticates a query for a secure computer network address, and the domain name database stores secure computer network addresses for the computer network. Each secure computer network address is based on a non-standard top-level domain name, such as .scom, .sorg, .snet, .snet, .sedu, .smil and .sint.

[0030] The present invention provides a way to encapsulate existing application network traffic at the application layer of a client computer so that the client application can securely communicate with a server protected by an agile network protocol. The advantages of the present invention are provided by a method for communicating using a private communication link between a client computer and a server computer over a computer network, such as the Internet. According to the invention, an information packet is sent from the client computer to the server computer over the computer network. The information packet contains data that is inserted into the payload portion of the packet at the application layer of the client computer and is used for forming a virtual private connection between the client computer and the server computer. The modified information packet can be sent through a firewall before being sent over the computer network to the server computer and by working on top of existing protocols (i.e., UDP, ICMP and TCP), the present invention more easily penetrates the firewall. The information packet is received at a kernel layer of an operating system on the server side. It is then determined at the kernel layer of the operating system on the host computer whether the information packet contains the data that is used for forming the virtual private connection. The server side replies by sending an information packet to the client computer that has been modified at the kernel layer to containing virtual private connection information in the payload portion of the reply information packet. Preferably, the information packet from the client computer and the reply information packet from the server side are each a UDP protocol information packet. Alternative, both information packets could be a TCP/IP protocol information packet, or an ICMP protocol information packet.

[0031] In accordance with one aspect of the invention, a network device comprises: a storage device storing an application program for a secure communications service; and at least one processor configured to execute the application program for the secure communications service so as to enable the network device to (a) send a request to look up a network address of a second network device based on an identifier associated with the second network device; (b) receive an indication that the second network device is available for the secure communications service, the indication including the requested network address of the second network device and provisioning information for a virtual private network communication link; (c) connect to the second network device, using the received network address of the second network device and the

Petitioner Apple Inc. - Exhibit 1002, p. 16

provisioning information for the virtual private network communication link; and (d) communicate with the second network device using the secure communications service via the virtual private network communication link.

[0032] In accordance with another aspect of the invention, A method executed by a first network device for communicating with a second network device, the method comprising: (a) sending a request to look up a network address of a second network device based on an identifier associated with the second network device; (b) receiving an indication that the second network device is available for a secure communications service, the indication including the requested network address of the second network device and provisioning information for a virtual private network communication link; (c) connecting to the second network device over the virtual private network communication link, using the received network address of the second network device and the provisioning information for the virtual private network communication link; and (d) communicating with the second network device using the secure communications service via the virtual private network communication link.

BRIEF DESCRIPTION OF THE DRAWINGS

[0033] FIG. 1 is an illustration of secure communications over the Internet according to a prior art embodiment.

[0034] FIG. 2 is an illustration of secure communications over the Internet according to an embodiment of the invention.

[0035] FIG. 3a is an illustration of a process of forming a tunneled IP packet according to an embodiment of the invention.

[0036] FIG. 3b is an illustration of a process of forming a tunneled IP packet according to another embodiment of the invention.

[0037] FIG. 4 is an illustration of an OSI layer location of processes that may be used to implement the invention.

Petitioner Apple Inc. - Exhibit 1002, p. 17

[0038] FIG. 5 is a flow chart illustrating a process for routing a tunneled packet according to an embodiment of the invention.

[0039] FIG. 6 is a flow chart illustrating a process for forming a tunneled packet according to an embodiment of the invention.

[0040] FIG. 7 is a flow chart illustrating a process for receiving a tunneled packet according to an embodiment of the invention.

[0041] FIG. 8 shows how a secure session is established and synchronized between a client and a TARP router.

[0042] FIG. 9 shows an IP address hopping scheme between a client computer and TARP router using transmit and receive tables in each computer.

[0043] FIG. 10 shows physical link redundancy among three Internet Service Providers (ISPs) and a client computer.

[0044] FIG. 11 shows how multiple IP packets can be embedded into a single "frame" such as an Ethernet frame, and further shows the use of a discriminator field to camouflage true packet recipients.

[0045] FIG. 12A shows a system that employs hopped hardware addresses, hopped IP addresses, and hopped discriminator fields.

[0046] FIG. 12B shows several different approaches for hopping hardware addresses, IP addresses, and discriminator fields in combination.

[0047] FIG. 13 shows a technique for automatically re-establishing synchronization between sender and receiver through the use of a partially public sync value.

[0048] FIG. 14 shows a "checkpoint" scheme for regaining synchronization between a sender and recipient.

[0049] FIG. 15 shows further details of the checkpoint scheme of FIG. 14.

Petitioner Apple Inc. - Exhibit 1002, p. 18

[0050] FIG. 16 shows how two addresses can be decomposed into a plurality of segments for comparison with presence vectors.

[0051] FIG. 17 shows a storage array for a receiver's active addresses.

[0052] FIG. 18 shows the receiver's storage array after receiving a sync request.

[0053] FIG. 19 shows the receiver's storage array after new addresses have been generated.

[0054] FIG. 20 shows a system employing distributed transmission paths.

[0055] FIG. 21 shows a plurality of link transmission tables that can be used to route packets in the system of FIG. 20.

[0056] FIG. 22A shows a flowchart for adjusting weight value distributions associated with a plurality of transmission links.

[0057] FIG. 22B shows a flowchart for setting a weight value to zero if a transmitter turns off.

[0058] FIG. 23 shows a system employing distributed transmission paths with adjusted weight value distributions for each path.

[0059] FIG. 24 shows an example using the system of FIG. 23.

[0060] FIG. 25 shows a conventional domain-name look-up service.

[0061] FIG. 26 shows a system employing a DNS proxy server with transparent VPN creation.

[0062] FIG. 27 shows steps that can be carried out to implement transparent VPN creation based on a DNS look-up function.

[0063] FIG. 28 shows a system including a link guard function that prevents packet overloading on a low-bandwidth link LOW BW.

Petitioner Apple Inc. - Exhibit 1002, p. 19

[0064] FIG. 29 shows one embodiment of a system employing the principles of FIG. 28.

[0065] FIG. 30 shows a system that regulates packet transmission rates by throttling the rate at which synchronizations are performed.

[0066] FIG. 31 shows a signaling server 3101 and a transport server 3102 used to establish a VPN with a client computer.

[0067] FIG. 32 shows message flows relating to synchronization protocols of FIG. 31.

[0068] FIG. 33 shows a system block diagram of a computer network in which the "one-click" secure communication link of the present invention is suitable for use.

[0069] FIG. 34 shows a flow diagram for installing and establishing a "one-click" secure communication link over a computer network according to the present invention.

[0070] FIG. 35 shows a flow diagram for registering a secure domain name according to the present invention.

[0071] FIG. 36 shows a system block diagram of a computer network in which a private connection according to the present invention can be configured to more easily traverse a firewall between two computer networks.

[0072] FIG. 37 shows a flow diagram for establishing a virtual private connection that is encapsulated using an existing network protocol.

DETAILED DESCRIPTION OF THE INVENTION

[0073] Referring to FIG. 2, a secure mechanism for communicating over the internet employs a number of special routers or servers, called TARP routers 122-127 that are similar to regular IP routers 128-132 in that each has one or more IP addresses and uses normal IP protocol to send normal-looking IP packet messages, called TARP packets 140. TARP packets 140 are

Petitioner Apple Inc. - Exhibit 1002, p. 20

identical to normal IP packet messages that are routed by regular IP routers 128-132 because each TARP packet 140 contains a destination address as in a normal IP packet. However, instead of indicating a final destination in the destination field of the IP header, the TARP packet's 140 IP header always points to a next-hop in a series of TARP router hops, or the final destination, TARP terminal 110. Because the header of the TARP packet contains only the next-hop destination, there is no overt indication from an intercepted TARP packet of the true destination of the TARP packet 140 since the destination could always be the next-hop TARP router as well as the final destination, TARP terminal 110.

[0074] Each TARP packet's true destination is concealed behind an outer layer of encryption generated using a link key 146. The link key 146 is the encryption key used for encrypted communication between the end points (TARP terminals or TARP routers) of a single link in the chain of hops connecting the originating TARP terminal 100 and the destination TARP terminal 110. Each TARP router 122-127, using the link key 146 it uses to communicate with the previous hop in a chain, can use the link key to reveal the true destination of a TARP packet. To identify the link key needed to decrypt the outer layer of encryption of a TARP packet, a receiving TARP or routing terminal may identify the transmitting terminal (which may indicate the link key used) by the sender field of the clear IP header. Alternatively, this identity may be hidden behind another layer of encryption in available bits in the clear IP header. Each TARP router, upon receiving a TARP message, determines if the message is a TARP message by using authentication data in the TARP packet. This could be recorded in available bytes in the TARP packet's IP header. Alternatively, TARP packets could be authenticated by attempting to decrypt using the link key 146 and determining if the results are as expected. The former may have computational advantages because it does not involve a decryption process.

[0075] Once the outer layer of decryption is completed by a TARP router 122-127, the TARP router determines the final destination. The system is preferably designed to cause each TARP packet 140 to undergo a minimum number of hops to help foil traffic analysis. The time to live counter in the IP header of the TARP message may be used to indicate a number of TARP router hops yet to be completed. Each TARP router then would decrement the counter and determine from that whether it should forward the TARP packet 140 to another TARP router

Petitioner Apple Inc. - Exhibit 1002, p. 21

122-127 or to the destination TARP terminal 110. If the time to live counter is zero or below zero after decrementing, for an example of usage, the TARP router receiving the TARP packet 140 may forward the TARP packet 140 to the destination TARP terminal 110. If the time to live counter is above zero after decrementing, for an example of usage, the TARP router receiving the TARP packet 140 may forward the TARP packet 140 to a TARP router 122-127 that the current TARP terminal chooses at random. As a result, each TARP packet 140 is routed through some minimum number of hops of TARP routers 122-127 which are chosen at random.

[0076] Thus, each TARP packet, irrespective of the traditional factors determining traffic in the Internet, makes random trips among a number of geographically disparate routers before reaching its destination and each trip is highly likely to be different for each packet composing a given message because each trip is independently randomly determined as described above. This feature is called *agile routing*. For reasons that will become clear shortly, the fact that different packets take different routes provides distinct advantages by making it difficult for an interloper to obtain all the packets forming an entire multi-packet message. Agile routing is combined with another feature that furthers this purpose, a feature that ensures that any message is broken into multiple packets.

[0077] A TARP router receives a TARP packet when an IP address used by the TARP router coincides with the IP address in the TARP packet's IP header IPc. The IP address of a TARP router, however, may not remain constant. To avoid and manage attacks, each TARP router, independently or under direction from another TARP terminal or router, may change its IP address. A separate, unchangeable identifier or address is also defined. This address, called the TARP address, is known only to TARP routers and terminals and may be correlated at any time by a TARP router or a TARP terminal using a Lookup Table (LUT). When a TARP router or terminal changes its IP address, it updates the other TARP routers and terminals which in turn update their respective LUTs. In reality, whenever a TARP router looks up the address of a destination in the encrypted header, it must convert a TARP address to a real IP address using its LUT.

[0078] While every TARP router receiving a TARP packet has the ability to determine the packet's final destination, the message payload is embedded behind an inner layer

Petitioner Apple Inc. - Exhibit 1002, p. 22

of encryption in the TARP packet that can only be unlocked using a session key. The session key is not available to any of the TARP routers 122-127 intervening between the originating 100 and destination 110 TARP terminals. The session key is used to decrypt the payloads of the TARP packets 140 permitting an entire message to be reconstructed.

[0079] In one embodiment, communication may be made private using link and session keys, which in turn may be shared and used according any desired method. For example, a public key or symmetric keys may be communicated between link or session endpoints using a public key method. Any of a variety of other mechanisms for securing data to ensure that only authorized computers can have access to the private information in the TARP packets 140 may be used as desired.

[0080] Referring to FIG. 3a, to construct a series of TARP packets, a data stream 300 of IP packets 207a, 207b, 207c, etc., such series of packets being formed by a network (IP) layer process, is broken into a series of small sized segments. In the present example, equal-sized segments 1-9 are defined and used to construct a set of interleaved data packets A, B, and C. Here it is assumed that the number of interleaved packets A, B, and C formed is three and that the number of IP packets 207a-207c used to form the three interleaved packets A, B, and C is exactly three. Of course, the number of IP packets spread over a group of interleaved packets may be any convenient number as may be the number of interleaved packets over which the incoming data stream is spread. The latter, the number of interleaved packets over which the data stream is spread, is called the *interleave window*.

[0081] To create a packet, the transmitting software interleaves the normal IP packets 207a *et. seq, to* form a new set of interleaved payload data 320. This payload data 320 is then encrypted using a session key to form a set of session-key-encrypted payload data 330, each of which, A, B, and C, will form the payload of a TARP packet. Using the IP header data, from the original packets 207a-207c, new TARP headers IPT are formed. The TARP headers IPT can be identical to normal IP headers or customized in some way. In a preferred embodiment, the TARP headers IPT are IP headers with added data providing the following information required for routing and reconstruction of messages, some of which data is ordinarily, or capable of being, contained in normal IP headers:

1. A window sequence number — an identifier that indicates where the packet belongs in the original message sequence.

2. An interleave sequence number — an identifier that indicates the interleaving sequence used to form the packet so that the packet can be deinterleaved along with other packets in the interleave window.

3. A time-to-live (TTL) datum — indicates the number of TARP-router-hops to be executed before the packet reaches its destination. Note that the TTL parameter may provide a datum to be used in a probabilistic formula for determining whether to route the packet to the destination or to another hop.

4. Data type identifier — indicates whether the payload contains, for example, TCP or UDP data.

5. Sender's address — indicates the sender's address in the TARP network.

6. Destination address — indicates the destination terminal's address in the TARP network.

7. Decoy/Real — an indicator of whether the packet contains real message data or dummy decoy data or a combination.

[0082] Obviously, the packets going into a single interleave window must include only packets with a common destination. Thus, it is assumed in the depicted example that the IP headers of IP packets 207a-207c all contain the same destination address or at least will be received by the same terminal so that they can be deinterleaved. Note that dummy or decoy data or packets can be added to form a larger interleave window than would otherwise be required by the size of a given message. Decoy or dummy data can be added to a stream to help foil traffic analysis by leveling the load on the network. Thus, it may be desirable to provide the TARP process with an ability to respond to the time of day or other criteria to generate more decoy data during low traffic periods so that communication bursts at one point in the Internet cannot be tied to communication bursts at another point to reveal the communicating endpoints.

Petitioner Apple Inc. - Exhibit 1002, p. 24

[0083] Dummy data also helps to break the data into a larger number of inconspicuously-sized packets permitting the interleave window size to be increased while maintaining a reasonable size for each packet. (The packet size can be a single standard size or selected from a fixed range of sizes.) One primary reason for desiring for each message to be broken into multiple packets is apparent if a chain block encryption scheme is used to form the first encryption layer prior to interleaving. A single block encryption may be applied to a portion, or the entirety, of a message, and that portion or entirety then interleaved into a number of separate packets.

[0084] Referring to FIG. 3b, in an alternative mode of TARP packet construction, a series of IP packets are accumulated to make up a predefined interleave window. The payloads of the packets are used to construct a single block 520 for chain block encryption using the session key. The payloads used to form the block are presumed to be destined for the same terminal. The block size may coincide with the interleave window as depicted in the example embodiment of FIG. 3b. After encryption, the encrypted block is broken into separate payloads and segments which are interleaved as in the embodiment of Fig 3a. The resulting interleaved packets A, B, and C, are then packaged as TARP packets with TARP headers as in the Example of FIG. 3a. The remaining process is as shown in, and discussed with reference to, FIG. 3a.

[0085] Once the TARP packets 340 are formed, each entire TARP packet 340, including the TARP header IPT, is encrypted using the link key for communication with the first-hop-TARP router. The first hop TARP router is randomly chosen. A final unencrypted IP header IPc is added to each encrypted TARP packet 340 to form a normal IP packet 360 that can be transmitted to a TARP router. Note that the process of constructing the TARP packet 360 does not have to be done in stages as described. The above description is just a useful heuristic for describing the final product, namely, the TARP packet.

[0086] Note that, TARP header IP_T could be a completely custom header configuration with no similarity to a normal IP header except that it contain the information identified above. This is so since this header is interpreted by only TARP routers.

[0087] The above scheme may be implemented entirely by processes operating between the data link layer and the network layer of each server or terminal participating in the TARP system. Referring to FIG. 4, a TARP transceiver 405 can be an originating terminal 100, a destination terminal 110, or a TARP router 122-127. In each TARP Transceiver 405, a transmitting process is generated to receive normal packets from the Network (IP) layer and generate TARP packets for communication over the network. A receiving process is generated to receive normal IP packets containing TARP packets and generate from these normal IP packets which are "passed up" to the Network (IP) layer. Note that where the TARP Transceiver 405 is a router, the received TARP packets 140 are not processed into a stream of IP packets 415 because they need only be authenticated as proper TARP packets and then passed to another TARP router or a TARP destination terminal 110. The intervening process, a "TARP Layer" 420, could be combined with either the data link layer 430 or the Network layer 410. In either case, it would intervene between the data link layer 430 so that the process would receive regular IP packets containing embedded TARP packets and "hand up" a series of reassembled IP packets to the Network layer 410. As an example of combining the TARP layer 420 with the data link layer 430, a program may augment the normal processes running a communications card, for example, an Ethernet card. Alternatively, the TARP layer processes may form part of a dynamically loadable module that is loaded and executed to support communications between the network and data link layers.

[0088] Because the encryption system described above can be inserted between the data link and network layers, the processes involved in supporting the encrypted communication may be completely transparent to processes at the IP (network) layer and above. The TARP processes may also be completely transparent to the data link layer processes as well. Thus, no operations at or above the network layer, or at or below the data link layer, are affected by the insertion of the TARP stack. This provides additional security to all processes at or above the network layer, since the difficulty of unauthorized penetration of the network layer (by, for example, a hacker) is increased substantially. Even newly developed servers running at the session layer leave all processes below the session layer vulnerable to attack. Note that in this architecture, security is distributed. That is, notebook computers used by executives on the road, for example, can communicate over the Internet without any compromise in security.

Petitioner Apple Inc. - Exhibit 1002, p. 26

[0089] Note that IP address changes made by TARP terminals and routers can be done at regular intervals, at random intervals, or upon detection of "attacks." The variation of IP addresses hinders traffic analysis that might reveal which computers are communicating, and also provides a degree of immunity from attack. The level of immunity from attack is roughly proportional to the rate at which the IP address of the host is changing.

[0090] As mentioned, IP addresses may be changed in response to attacks. An attack may be revealed, for example, by a regular series of messages indicates that a router is being probed in some way. Upon detection of an attack, the TARP layer process may respond to this event by changing its IP address. To accomplish this, the TARP process will construct a TARP-formatted message, in the style of Internet Control Message Protocol (ICMP) datagrams as an example; this message will contain the machine's TARP address, its previous IP address, and its new IP address. The TARP layer will transmit this packet to at least one known TARP router; then upon receipt and validation of the message, the TARP router will update its LUT with the new IP address for the stated TARP address. The TARP router will then format a similar message, and broadcast it to the other TARP routers so that they may update their LUTs. Since the total number of TARP routers on any given subnet is expected to be relatively small, this process of updating the LUTs should be relatively fast. It may not, however, work as well when there is a relatively large number of TARP routers and/or a relatively large number of clients; this has motivated a refinement of this architecture to provide scalability; this refinement has led to a second embodiment, which is discussed below.

[0091] Upon detection of an attack, the TARP process may also create a subprocess that maintains the original IP address and continues interacting with the attacker. The latter may provide an opportunity to trace the attacker or study the attacker's methods (called "fishbowling" drawing upon the analogy of a small fish in a fish bowl that "thinks" it is in the ocean but is actually under captive observation). A history of the communication between the attacker and the abandoned (fishbowled) IP address can be recorded or transmitted for human analysis or further synthesized for purposes of responding in some way.

[0092] As mentioned above, decoy or dummy data or packets can be added to outgoing data streams by TARP terminals or routers. In addition to making it convenient to

Petitioner Apple Inc. - Exhibit 1002, p. 27

spread data over a larger number of separate packets, such decoy packets can also help to level the load on inactive portions of the Internet to help foil traffic analysis efforts.

[0093] Decoy packets may be generated by each TARP terminal 100, 110 or each router 122-127 on some basis determined by an algorithm. For example, the algorithm may be a random one which calls for the generation of a packet on a random basis when the terminal is idle. Alternatively, the algorithm may be responsive to time of day or detection of low traffic to generate more decoy packets during low traffic times. Note that packets are preferably generated in groups, rather than one by one, the groups being sized to simulate real messages. In addition, so that decoy packets may be inserted in normal TARP message streams, the background loop may have a latch that makes it more likely to insert decoy packets when a message stream is being received. That is, when a series of messages are received, the decoy packet generation rate may be increased. Alternatively, if a large number of decoy packets is received along with regular TARP packets, the algorithm may increase the rate of dropping of decoy packets rather than forwarding them. The result of dropping and generating decoy packets in this way is to make the apparent incoming message size different from the apparent outgoing message size to help foil traffic analysis. The rate of reception of packets, decoy or otherwise, may be indicated to the decoy packet dropping and generating processes through perishable decoy and regular packet counters. (A perishable counter is one that resets or decrements its value in response to time so that it contains a high value when it is incremented in rapid succession and a small value when incremented either slowly or a small number of times in rapid succession.) Note that destination TARP terminal 110 may generate decoy packets equal in number and size to those TARP packets received to make it appear it is merely routing packets and is therefore not the destination terminal.

[0094] Referring to FIG. 5, the following particular steps may be employed in the above- described method for routing TARP packets.

- S0. A background loop operation is performed which applies an algorithm which determines the generation of decoy IP packets. The loop is interrupted when an encrypted TARP packet is received.

Petitioner Apple Inc. - Exhibit 1002, p. 28

- S2. The TARP packet may be probed in some way to authenticate the packet before attempting to decrypt it using the link key. That is, the router may determine that the packet is an authentic TARP packet by performing a selected operation on some data included with the clear IP header attached to the encrypted TARP packet contained in the payload. This makes it possible to avoid performing decryption on packets that are not authentic TARP packets.

- S3. The TARP packet is decrypted to expose the destination TARP address and an indication of whether the packet is a decoy packet or part of a real message.

- S4. If the packet is a decoy packet, the perishable decoy counter is incremented.

- S5. Based on the decoy generation/dropping algorithm and the perishable decoy counter value, if the packet is a decoy packet, the router may choose to throw it away. If the received packet is a decoy packet and it is determined that it should be thrown away (S6), control returns to step S0.

- S7. The TTL parameter of the TARP header is decremented and it is determined if the TTL parameter is greater than zero.

- S8. If the TTL parameter is greater than zero, a TARP address is randomly chosen from a list of TARP addresses maintained by the router and the link key and IP address corresponding to that TARP address memorized for use in creating a new IP packet containing the TARP packet.

- S9. If the TTL parameter is zero or less, the link key and IP address corresponding to the TARP address of the destination are memorized for use in creating the new IP packet containing the TARP packet.

- S 10. The TARP packet is encrypted using the memorized link key.

- S 11. An IP header is added to the packet that contains the stored IP address, the encrypted TARP packet wrapped with an IP header, and the completed packet transmitted to the next hop or destination.

Petitioner Apple Inc. - Exhibit 1002, p. 29

[0095] Referring to FIG. 6, the following particular steps may be employed in the above- described method for generating TARP packets.

- S20. A background loop operation applies an algorithm that determines the generation of decoy IP packets. The loop is interrupted when a data stream containing IP packets is received for transmission.

- S21. The received IP packets are grouped into a set consisting of messages with a constant IP destination address. The set is further broken down to coincide with a maximum size of an interleave window The set is encrypted, and interleaved into a set of payloads destined to become TARP packets.

- S22. The TARP address corresponding to the IP address is determined from a lookup table and stored to generate the TARP header. An initial TTL count is generated and stored in the header. The TTL count may be random with minimum and maximum values or it may be fixed or determined by some other parameter.

- S23. The window sequence numbers and interleave sequence numbers are recorded in the TARP headers of each packet.

- S24. One TARP router address is randomly chosen for each TARP packet and the IP address corresponding to it stored for use in the clear IP header. The link key corresponding to this router is identified and used to encrypt TARP packets containing interleaved and encrypted data and TARP headers.

- S25. A clear IP header with the first hop router's real IP address is generated and added to each of the encrypted TARP packets and the resulting packets.

[0096] Referring to FIG. 7, the following particular steps may be employed in the above- described method for receiving TARP packets.

- S40. A background loop operation is performed which applies an algorithm which determines the generation of decoy IP packets. The loop is interrupted when an encrypted TARP packet is received.

Petitioner Apple Inc. - Exhibit 1002, p. 30

- S42. The TARP packet may be probed to authenticate the packet before attempting to decrypt it using the link key.
- S43. The TARP packet is decrypted with the appropriate link key to expose the destination TARP address and an indication of whether the packet is a decoy packet or part of a real message.
- S44. If the packet is a decoy packet, the perishable decoy counter is incremented.
- S45. Based on the decoy generation/dropping algorithm and the perishable decoy counter value, if the packet is a decoy packet, the receiver may choose to throw it away.
- S46. The TARP packets are cached until all packets forming an interleave window are received.
- S47. Once all packets of an interleave window are received, the packets are deinterleaved.
- S48. The packets block of combined packets defining the interleave window is then decrypted using the session key.
- S49. The decrypted block is then divided using the window sequence data and the IP_T headers are converted into normal IP_C headers. The window sequence numbers are integrated in the IP_C headers.
- S50. The packets are then handed up to the IP layer processes.

1. SCALABILITY ENHANCEMENTS

[0097] The IP agility feature described above relies on the ability to transmit IP address changes to all TARP routers. The embodiments including this feature will be referred to as "boutique" embodiments due to potential limitations in scaling these features up for a large network, such as the Internet. (The "boutique" embodiments would, however, be robust for use in smaller networks, such as small virtual private networks, for example). One problem with the boutique embodiments is that if IP address changes are to occur frequently, the message traffic

required to update all routers sufficiently quickly creates a serious burden on the Internet when the TARP router and/or client population gets large. The bandwidth burden added to the networks, for example in ICMP packets, that would be used to update all the TARP routers could overwhelm the Internet for a large scale implementation that approached the scale of the Internet. In other words, the boutique system's scalability is limited.

[0098] A system can be constructed which trades some of the features of the above embodiments to provide the benefits of IP agility without the additional messaging burden. This is accomplished by IP address-hopping according to shared algorithms that govern IP addresses used between links participating in communications sessions between nodes such as TARP nodes. (Note that the IP hopping technique is also applicable to the boutique embodiment.) The IP agility feature discussed with respect to the boutique system can be modified so that it becomes decentralized under this scalable regime and governed by the above-described shared algorithm. Other features of the boutique system may be combined with this new type of IP-agility.

[0099] The new embodiment has the advantage of providing IP agility governed by a local algorithm and set of IP addresses exchanged by each communicating pair of nodes. This local governance is session-independent in that it may govern communications between a pair of nodes, irrespective of the session or end points being transferred between the directly communicating pair of nodes.

[00100] In the scalable embodiments, blocks of IP addresses are allocated to each node in the network. (This scalability will increase in the future, when Internet Protocol addresses are increased to 128-bit fields, vastly increasing the number of distinctly addressable nodes). Each node can thus use any of the IP addresses assigned to that node to communicate with other nodes in the network. Indeed, each pair of communicating nodes can use a plurality of source IP addresses and destination IP addresses for communicating with each other.

[00101] Each communicating pair of nodes in a chain participating in any session stores two blocks of IP addresses, called netblocks, and an algorithm and randomization seed for selecting, from each netblock, the next pair of source/destination IP addresses that will be used to

Petitioner Apple Inc. - Exhibit 1002, p. 32

transmit the next message. In other words, the algorithm governs the sequential selection of IP-address pairs, one sender and one receiver IP address, from each netblock. The combination of algorithm, seed, and netblock (IP address block) will be called a "hopblock." A router issues separate transmit and receive hopblocks to its clients. The send address and the receive address of the IP header of each outgoing packet sent by the client are filled with the send and receive IP addresses generated by the algorithm. The algorithm is "clocked" (indexed) by a counter so that each time a pair is used, the algorithm turns out a new transmit pair for the next packet to be sent.

[00102] The router's receive hopblock is identical to the client's transmit hopblock. The router uses the receive hopblock to predict what the send and receive IP address pair for the next expected packet from that client will be. Since packets can be received out of order, it is not possible for the router to predict with certainty what IP address pair will be on the next sequential packet. To account for this problem, the router generates a range of predictions encompassing the number of possible transmitted packet send/receive addresses, of which the next packet received could leap ahead. Thus, if there is a vanishingly small probability that a given packet will arrive at the router ahead of 5 packets transmitted by the client before the given packet, then the router can generate a series of 6 send/receive IP address pairs (or "hop window") to compare with the next received packet. When a packet is received, it is marked in the hop window as such, so that a second packet with the same IP address pair will be discarded. If an out-of-sequence packet does not arrive within a predetermined timeout period, it can be requested for retransmission or simply discarded from the receive table, depending upon the protocol in use for that communications session, or possibly by convention.

[00103] When the router receives the client's packet, it compares the send and receive IP addresses of the packet with the next N predicted send and receive IP address pairs and rejects the packet if it is not a member of this set. Received packets that do not have the predicted source/destination IP addresses falling with the window are rejected, thus thwarting possible hackers. (With the number of possible combinations, even a fairly large window would be hard to fall into at random.) If it is a member of this set, the router accepts the packet and processes it further. This link-based IP-hopping strategy, referred to as "IHOP," is a network element that stands on its own and is not necessarily accompanied by elements of the boutique system

Petitioner Apple Inc. - Exhibit 1002, p. 33

described above. If the routing agility feature described in connection with the boutique embodiment is combined with this link-based IP-hopping strategy, the router's next step would be to decrypt the TARP header to determine the destination TARP router for the packet and determine what should be the next hop for the packet. The TARP router would then forward the packet to a random TARP router or the destination TARP router with which the source TARP router has a link-based IP hopping communication established.

[00104] Figure 8 shows how a client computer 801 and a TARP router 811 can establish a secure session. When client 801 seeks to establish an IHOP session with TARP router 811, the client 801 sends "secure synchronization" request ("SSYN") packet 821 to the TARP router 811. This SYN packet 821 contains the client's 801 authentication token, and may be sent to the router 811 in an encrypted format. The source and destination IP numbers on the packet 821 are the client's 801 current fixed IP address, and a "known" fixed IP address for the router 811. (For security purposes, it may be desirable to reject any packets from outside of the local network that are destined for the router's known fixed IP address.) Upon receipt and validation of the client's 801 SSYN packet 821, the router 811 responds by sending an encrypted "secure synchronization acknowledgment" ("SSYN ACK") 822 to the client 801. This SSYN ACK 822 will contain the transmit and receive hopblocks that the client 801 will use when communicating with the TARP router 811. The client 801 will acknowledge the TARP router's 811 response packet 822 by generating an encrypted SSYN ACK ACK packet 823 which will be sent from the client's 801 fixed IP address and to the TARP router's 811 known fixed IP address. The client 801 will simultaneously generate a SSYN ACK ACK packet; this SSYN ACK packet, referred to as the Secure Session Initiation (SSI) packet 824, will be sent with the first {sender, receiver} IP pair in the client's transmit table 921 (FIG. 9), as specified in the transmit hopblock provided by the TARP router 811 in the SSYN ACK packet 822. The TARP router 811 will respond to the SSI packet 824 with an SSI ACK packet 825, which will be sent with the first {sender, receiver} IP pair in the TARP router's transmit table 923. Once these packets have been successfully exchanged, the secure communications session is established, and all further secure communications between the client 801 and the TARP router 811 will be conducted via this secure session, as long as synchronization is maintained. If synchronization is lost, then the client

Petitioner Apple Inc. - Exhibit 1002, p. 34

801 and TARP router 802 may re-establish the secure session by the procedure outlined in Figure 8 and described above.

[00105] While the secure session is active, both the client 901 and TARP router 911 (FIG. 9) will maintain their respective transmit tables 921, 923 and receive tables 922, 924, as provided by the TARP router during session synchronization 822. It is important that the sequence of IP pairs in the client's transmit table 921 be identical to those in the TARP router's receive table 924; similarly, the sequence of IP pairs in the client's receive table 922 must be identical to those in the router's transmit table 923. This is required for the session synchronization to be maintained. The client 901 need maintain only one transmit table 921 and one receive table 922 during the course of the secure session. Each sequential packet sent by the client 901 will employ the next {send, receive} IP address pair in the transmit table, regardless of TCP or UDP session. The TARP router 911 will expect each packet arriving from the client 901 to bear the next IP address pair shown in its receive table.

[00106] Since packets can arrive out of order, however, the router 911 can maintain a "look ahead" buffer in its receive table, and will mark previously-received IP pairs as invalid for future packets; any future packet containing an IP pair that is in the look-ahead buffer but is marked as previously received will be discarded. Communications from the TARP router 911 to the client 901 are maintained in an identical manner; in particular, the router 911 will select the next IP address pair from its transmit table 923 when constructing a packet to send to the client 901, and the client 901 will maintain a look-ahead buffer of expected IP pairs on packets that it is receiving. Each TARP router will maintain separate pairs of transmit and receive tables for each client that is currently engaged in a secure session with or through that TARP router.

[00107] While clients receive their hopblocks from the first server linking them to the Internet, routers exchange hopblocks. When a router establishes a link-based IP-hopping communication regime with another router, each router of the pair exchanges its transmit hopblock. The transmit hopblock of each router becomes the receive hopblock of the other router. The communication between routers is governed as described by the example of a client sending a packet to the first router.

Petitioner Apple Inc. - Exhibit 1002, p. 35

[00108] While the above strategy works fine in the IP milieu, many local networks that are connected to the Internet are Ethernet systems. In Ethernet, the IP addresses of the destination devices must be translated into hardware addresses, and vice versa, using known processes ("address resolution protocol," and "reverse address resolution protocol"). However, if the link- based IP-hopping strategy is employed, the correlation process would become explosive and burdensome. An alternative to the link-based IP hopping strategy may be employed within an Ethernet network. The solution is to provide that the node linking the Internet to the Ethernet (call it the border node) use the link-based IP-hopping communication regime to communicate with nodes outside the Ethernet LAN. Within the Ethernet LAN, each TARP node would have a single IP address which would be addressed in the conventional way. Instead of comparing the {sender, receiver} IP address pairs to authenticate a packet, the intra-LAN TARP node would use one of the IP header extension fields to do so. Thus, the border node uses an algorithm shared by the intra-LAN TARP node to generate a symbol that is stored in the free field in the IP header, and the intra-LAN TARP node generates a range of symbols based on its prediction of the next expected packet to be received from that particular source IP address. The packet is rejected if it does not fall into the set of predicted symbols (for example, numerical values) or is accepted if it does. Communications from the intra-LAN TARP node to the border node are accomplished in the same manner, though the algorithm will necessarily be different for security reasons. Thus, each of the communicating nodes will generate transmit and receive tables in a similar manner to that of Figure 9; the intra-LAN TARP nodes transmit table will be identical to the border node's receive table, and the intra-LAN TARP node's receive table will be identical to the border node's transmit table.

[00109] The algorithm used for IP address-hopping can be any desired algorithm. For example, the algorithm can be a given pseudo-random number generator that generates numbers of the range covering the allowed IP addresses with a given seed. Alternatively, the session participants can assume a certain type of algorithm and specify simply a parameter for applying the algorithm. For example the assumed algorithm could be a particular pseudo-random number generator and the session participants could simply exchange seed values.

Petitioner Apple Inc. - Exhibit 1002, p. 36

[00110] Note that there is no permanent physical distinction between the originating and destination terminal nodes. Either device at either end point can initiate a synchronization of the pair. Note also that the authentication/synchronization-request (and acknowledgment) and hopblock-exchange may all be served by a single message so that separate message exchanges may not be required.

[00111] As another extension to the stated architecture, multiple physical paths can be used by a client, in order to provide link redundancy and further thwart attempts at denial of service and traffic monitoring. As shown in Figure 10, for example, client 1001 can establish three simultaneous sessions with each of three TARP routers provided by different ISPs 1011, 1012, 1013. As an example, the client 1001 can use three different telephone lines 1021, 1022, 1023 to connect to the ISPs, or two telephone lines and a cable modem, etc. In this scheme, transmitted packets will be sent in a random fashion among the different physical paths. This architecture provides a high degree of communications redundancy, with improved immunity from denial-of- service attacks and traffic monitoring.

2. FURTHER EXTENSIONS

[00112] The following describes various extensions to the techniques, systems, and methods described above. As described above, the security of communications occurring between computers in a computer network (such as the Internet, an Ethernet, or others) can be enhanced by using seemingly random source and destination Internet Protocol (IP) addresses for data packets transmitted over the network. This feature prevents eavesdroppers from determining which computers in the network are communicating with each other while permitting the two communicating computers to easily recognize whether a given received data packet is legitimate or not. In one embodiment of the above-described systems, an IP header extension field is used to authenticate incoming packets on an Ethernet.

[00113] Various extensions to the previously described techniques described herein include: (1) use of hopped hardware or "MAC" addresses in broadcast type network; (2) a self synchronization technique that permits a computer to automatically regain synchronization with a sender; (3) synchronization algorithms that allow transmitting and receiving computers to

quickly re-establish synchronization in the event of lost packets or other events; and (4) a fast-packet rejection mechanism for rejecting invalid packets. Any or all of these extensions can be combined with the features described above in any of various ways.

A. Hardware Address Hopping

[00114] Internet protocol-based communications techniques on a LAN—or across any dedicated physical medium—typically embed the IP packets within lower-level packets, often referred to as "frames." As shown in FIG. 11, for example, a first Ethernet frame 1150 comprises a frame header 1101 and two embedded IP packets IP1 and IP2, while a second Ethernet frame 1160 comprises a different frame header 1104 and a single IP packet IP3. Each frame header generally includes a source hardware address 1101 A and a destination hardware address 1101 B; other well-known fields in frame headers are omitted from FIG. 11 for clarity. Two hardware nodes communicating over a physical communication channel insert appropriate source and destination hardware addresses to indicate which nodes on the channel or network should receive the frame.

[00115] It may be possible for a nefarious listener to acquire information about the contents of a frame and/or its communicants by examining frames on a local network rather than (or in addition to) the IP packets themselves. This is especially true in broadcast media, such as Ethernet, where it is necessary to insert into the frame header the hardware address of the machine that generated the frame and the hardware address of the machine to which frame is being sent. All nodes on the network can potentially "see" all packets transmitted across the network. This can be a problem for secure communications, especially in cases where the communicants do not want for any third party to be able to identify who is engaging in the information exchange. One way to address this problem is to push the address-hopping scheme down to the hardware layer. In accordance with various embodiments of the invention, hardware addresses are "hopped" in a manner similar to that used to change IP addresses, such that a listener cannot determine which hardware node generated a particular message nor which node is the intended recipient.

Petitioner Apple Inc. - Exhibit 1002, p. 38

[00116] FIG. 12A shows a system in which Media Access Control ("MAC") hardware addresses are "hopped" in order to increase security over a network such as an Ethernet. While the description refers to the exemplary case of an Ethernet environment, the inventive principles are equally applicable to other types of communications media. In the Ethernet case, the MAC address of the sender and receiver are inserted into the Ethernet frame and can be observed by anyone on the LAN who is within the broadcast range for that frame. For secure communications, it becomes desirable to generate frames with MAC addresses that are not attributable to any specific sender or receiver.

[00117] As shown in FIG. 12A, two computer nodes 1201 and 1202 communicate over a communication channel such as an Ethernet. Each node executes one or more application programs 1203 and 1218 that communicate by transmitting packets through communication software 1204 and 1217, respectively. Examples of application programs include video conferencing, e-mail, word processing programs, telephony, and the like. Communication software 1204 and 1217 can comprise, for example, an OSI layered architecture or "stack" that standardizes various services provided at different levels of functionality.

[00118] The lowest levels of communication software 1204 and 1217 communicate with hardware components 1206 and 1214 respectively, each of which can include one or more registers 1207 and 1215 that allow the hardware to be reconfigured or controlled in accordance with various communication protocols. The hardware components (an Ethernet network interface card, for example) communicate with each other over the communication medium. Each hardware component is typically pre-assigned a fixed hardware address or MAC number that identifies the hardware component to other nodes on the network. One or more interface drivers control the operation of each card and can, for example, be configured to accept or reject packets from certain hardware addresses. As will be described in more detail below, various embodiments of the inventive principles provide for "hopping" different addresses using one or more algorithms and one or more moving windows that track a range of valid addresses to validate received packets. Packets transmitted according to one or more of the inventive principles will be generally referred to as "secure" packets or "secure communications" to

Petitioner Apple Inc. - Exhibit 1002, p. 39

differentiate them from ordinary data packets that are transmitted in the clear using ordinary, machine-correlated addresses.

[00119] One straightforward method of generating non-attributable MAC addresses is an extension of the IP hopping scheme. In this scenario, two machines on the same LAN that desire to communicate in a secure fashion exchange random-number generators and seeds, and create sequences of quasi-random MAC addresses for synchronized hopping. The implementation and synchronization issues are then similar to that of IP hopping.

[00120] This approach, however, runs the risk of using MAC addresses that are currently active on the LAN—which, in turn, could interrupt communications for those machines. Since an Ethernet MAC address is at present 48 bits in length, the chance of randomly misusing an active MAC address is actually quite small. However, if that figure is multiplied by a large number of nodes (as would be found on an extensive LAN), by a large number of frames (as might be the case with packet voice or streaming video), and by a large number of concurrent Virtual Private Networks (VPNs), then the chance that a non-secure machine's MAC address could be used in an address-hopped frame can become non-trivial. In short, any scheme that runs even a small risk of interrupting communications for other machines on the LAN is bound to receive resistance from prospective system administrators. Nevertheless, it is technically feasible, and can be implemented without risk on a LAN on which there is a small number of machines, or if all of the machines on the LAN are engaging in MAC-hopped communications.

[00121] Synchronized MAC address hopping may incur some overhead in the course of session establishment, especially if there are multiple sessions or multiple nodes involved in the communications. A simpler method of randomizing MAC addresses is to allow each node to receive and process every incident frame on the network. Typically, each network interface driver will check the destination MAC address in the header of every incident frame to see if it matches that machine's MAC address; if there is no match, then the frame is discarded. In one embodiment, however, these checks can be disabled, and every incident packet is passed to the TARP stack for processing. This will be referred to as "promiscuous" mode, since every incident frame is processed. Promiscuous mode allows the sender to use completely random, unsynchronized MAC addresses, since the destination machine is guaranteed to process the

Petitioner Apple Inc. - Exhibit 1002, p. 40

frame. The decision as to whether the packet was truly intended for that machine is handled by the TARP stack, which checks the source and destination IP addresses for a match in its IP synchronization tables. If no match is found, the packet is discarded; if there is a match, the packet is unwrapped, the inner header is evaluated, and if the inner header indicates that the packet is destined for that machine then the packet is forwarded to the IP stack—otherwise it is discarded.

[00122] One disadvantage of purely-random MAC address hopping is its impact on processing overhead; that is, since every incident frame must be processed, the machine's CPU is engaged considerably more often than if the network interface driver is discriminating and rejecting packets unilaterally. A compromise approach is to select either a single fixed MAC address or a small number of MAC addresses (e.g., one for each virtual private network on an Ethernet) to use for MAC-hopped communications, regardless of the actual recipient for which the message is intended. In this mode, the network interface driver can check each incident frame against one (or a few) pre-established MAC addresses, thereby freeing the CPU from the task of physical- layer packet discrimination. This scheme does not betray any useful information to an interloper on the LAN; in particular, every secure packet can already be identified by a unique packet type in the outer header. However, since all machines engaged in secure communications would either be using the same MAC address, or be selecting from a small pool of predetermined MAC addresses, the association between a specific machine and a specific MAC address is effectively broken.

[00123] In this scheme, the CPU will be engaged more often than it would be in non-secure communications (or in synchronized MAC address hopping), since the network interface driver cannot always unilaterally discriminate between secure packets that are destined for that machine, and secure packets from other VPNs. However, the non-secure traffic is easily eliminated at the network interface, thereby reducing the amount of processing required of the CPU. There are boundary conditions where these statements would not hold, of course—e.g., if all of the traffic on the LAN is secure traffic, then the CPU would be engaged to the same degree as it is in the purely-random address hopping case; alternatively, if each VPN on the LAN uses a different MAC address, then the network interface can perfectly discriminate secure frames

destined for the local machine from those constituting other VPNs. These are engineering tradeoffs that might be best handled by providing administrative options for the users when installing the software and/or establishing VPNs.

[00124] Even in this scenario, however, there still remains a slight risk of selecting MAC addresses that are being used by one or more nodes on the LAN. One solution to this problem is to formally assign one address or a range of addresses for use in MAC-hopped communications. This is typically done via an assigned numbers registration authority; e.g., in the case of Ethernet, MAC address ranges are assigned to vendors by the Institute of Electrical and Electronics Engineers (IEEE). A formally-assigned range of addresses would ensure that secure frames do not conflict with any properly-configured and properly-functioning machines on the LAN.

[00125] Reference will now be made to FIGS. 12A and 12B in order to describe the many combinations and features that follow the inventive principles. As explained above, two computer nodes 1201 and 1202 are assumed to be communicating over a network or communication medium such as an Ethernet. A communication protocol in each node (1204 and 1217, respectively) contains a modified element 1205 and 1216 that performs certain functions that deviate from the standard communication protocols. In particular, computer node 1201 implements a first "hop" algorithm 1208X that selects seemingly random source and destination IP addresses (and, in one embodiment, seemingly random IP header discriminator fields) in order to transmit each packet to the other computer node. For example, node 1201 maintains a transmit table 1208 containing triplets of source (S), destination (D), and discriminator fields (DS) that are inserted into outgoing IP packet headers. The table is generated through the use of an appropriate algorithm (e.g., a random number generator that is seeded with an appropriate seed) that is known to the recipient node 1202. As each new IP packet is formed, the next sequential entry out of the sender's transmit table 1208 is used to populate the IP source, IP destination, and IP header extension field (e.g., discriminator field). It will be appreciated that the transmit table need not be created in advance but could instead be created on-the-fly by executing the algorithm when each packet is formed.

Petitioner Apple Inc. - Exhibit 1002, p. 42

[00126] At the receiving node 1202, the same IP hop algorithm 1222X is maintained and used to generate a receive table 1222 that lists valid triplets of source IP address, destination IP address, and discriminator field. This is shown by virtue of the first five entries of transmit table 1208 matching the second five entries of receive table 1222. (The tables may be slightly offset at any particular time due to lost packets, misordered packets, or transmission delays). Additionally, node 1202 maintains a receive window W3 that represents a list of valid IP source, IP destination, and discriminator fields that will be accepted when received as part of an incoming IP packet. As packets are received, window W3 slides down the list of valid entries, such that the possible valid entries change over time. Two packets that arrive out of order but are nevertheless matched to entries within window W3 will be accepted; those falling outside of window W3 will be rejected as invalid. The length of window W3 can be adjusted as necessary to reflect network delays or other factors.

[00127] Node 1202 maintains a similar transmit table 1221 for creating IP packets and frames destined for node 1201 using a potentially different hopping algorithm 1221 X, and node 1201 maintains a matching receive table 1209 using the same algorithm 1209X. As node 1202 transmits packets to node 1201 using seemingly random IP source, IP destination, and/or discriminator fields, node 1201 matches the incoming packet values to those falling within window WI maintained in its receive table. In effect, transmit table 1208 of node 1201 is synchronized (i.e., entries are selected in the same order) to receive table 1222 of receiving node 1202. Similarly, transmit table 1221 of node 1202 is synchronized to receive table 1209 of node 1201. It will be appreciated that although a common algorithm is shown for the source, destination and discriminator fields in FIG. 12A (using, e.g., a different seed for each of the three fields), an entirely different algorithm could in fact be used to establish values for each of these fields. It will also be appreciated that one or two of the fields can be "hopped" rather than all three as illustrated.

[00128] In accordance with another aspect of the invention, hardware or "MAC" addresses are hopped instead of or in addition to IP addresses and/or the discriminator field in order to improve security in a local area or broadcast-type network. To that end, node 1201 further maintains a transmit table 1210 using a transmit algorithm 1210X to generate source and

destination hardware addresses that are inserted into frame headers (e.g., fields 1101A and 1101 B in FIG. 11) that are synchronized to a corresponding receive table 1224 at node 1202. Similarly, node 1202 maintains a different transmit table 1223 containing source and destination hardware addresses that is synchronized with a corresponding receive table 1211 at node 1201. In this manner, outgoing hardware frames appear to be originating from and going to completely random nodes on the network, even though each recipient can determine whether a given packet is intended for it or not. It will be appreciated that the hardware hopping feature can be implemented at a different level in the communications protocol than the IP hopping feature (e.g., in a card driver or in a hardware card itself to improve performance).

[00129] FIG. 12B shows three different embodiments or modes that can be employed using the aforementioned principles. In a first mode referred to as "promiscuous" mode, a common hardware address (e.g., a fixed address for source and another for destination) or else a completely random hardware address is used by all nodes on the network, such that a particular packet cannot be attributed to any one node. Each node must initially accept all packets containing the common (or random) hardware address and inspect the IP addresses or discriminator field to determine whether the packet is intended for that node. In this regard, either the IP addresses or the discriminator field or both can be varied in accordance with an algorithm as described above. As explained previously, this may increase each node's overhead since additional processing is involved to determine whether a given packet has valid source and destination hardware addresses.

[00130] In a second mode referred to as "promiscuous per VPN" mode, a small set of fixed hardware addresses are used, with a fixed source/destination hardware address used for all nodes communicating over a virtual private network. For example, if there are six nodes on an Ethernet, and the network is to be split up into two private virtual networks such that nodes on one VPN can communicate with only the other two nodes on its own VPN, then two sets of hardware addresses could be used: one set for the first VPN and a second set for the second VPN. This would reduce the amount of overhead involved in checking for valid frames since only packets arriving from the designated VPN would need to be checked. IP addresses and one or more discriminator fields could still be hopped as before for secure communication within the

Petitioner Apple Inc. - Exhibit 1002, p. 44

VPN. Of course, this solution compromises the anonymity of the VPNs (i.e., an outsider can easily tell what traffic belongs in which VPN, though he cannot correlate it to a specific machine/person). It also requires the use of a discriminator field to mitigate the vulnerability to certain types of DoS attacks, (For example, without the discriminator field, an attacker on the LAN could stream frames containing the MAC addresses being used by the VPN; rejecting those frames could lead to excessive processing overhead. The discriminator field would provide a low-overhead means of rejecting the false packets.)

[00131] In a third mode referred to as "hardware hopping" mode, hardware addresses are varied as illustrated in FIG. 12A, such that hardware source and destination addresses are changed constantly in order to provide non-attributable addressing. Variations on these embodiments are of course possible, and the invention is not intended to be limited in any respect by these illustrative examples.

B. Extending the Address Space

[00132] Address hopping provides security and privacy. However, the level of protection is limited by the number of addresses in the blocks being hopped. A hopblock denotes a field or fields modulated on a packet-wise basis for the purpose of providing a VPN. For instance, if two nodes communicate with IP address hopping using hopblocks of 4 addresses (2 bits) each, there would be 16 possible address-pair combinations. A window of size 16 would result in most address pairs being accepted as valid most of the time. This limitation can be overcome by using a discriminator field in addition to or instead of the hopped address fields. The discriminator field would be hopped in exactly the same fashion as the address fields and it would be used to determine whether a packet should be processed by a receiver.

[00133] Suppose that two clients, each using four-bit hopblocks, would like the same level of protection afforded to clients communicating via IP hopping between two A blocks (24 address bits eligible for hopping). A discriminator field of 20 bits, used in conjunction with the 4 address bits eligible for hopping in the IP address field, provides this level of protection. A 24-bit discriminator field would provide a similar level of protection if the address fields were not hopped or ignored. Using a discriminator field offers the following advantages: (1) an arbitrarily

high level of protection can be provided, and (2) address hopping is unnecessary to provide protection. This may be important in environments where address hopping would cause routing problems.

C. Synchronization Techniques

[00134] It is generally assumed that once a sending node and receiving node have exchanged algorithms and seeds (or similar information sufficient to generate quasi-random source and destination tables), subsequent communication between the two nodes will proceed smoothly. Realistically, however, two nodes may lose synchronization due to network delays or outages, or other problems. Consequently, it is desirable to provide means for re-establishing synchronization between nodes in a network that have lost synchronization.

[00135] One possible technique is to require that each node provide an acknowledgment upon successful receipt of each packet and, if no acknowledgment is received within a certain period of time, to re-send the unacknowledged packet. This approach, however, drives up overhead costs and may be prohibitive in high-throughput environments such as streaming video or audio, for example.

[00136] A different approach is to employ an automatic synchronizing technique that will be referred to herein as "self-synchronization." In this approach, synchronization information is embedded into each packet, thereby enabling the receiver to re-synchronize itself upon receipt of a single packet if it determines that is has lost synchronization with the sender. (If communications are already in progress, and the receiver determines that it is still in sync with the sender, then there is no need to re-synchronize.) A receiver could detect that it was out of synchronization by, for example, employing a "dead-man" timer that expires after a certain period of time, wherein the timer is reset with each valid packet. A time stamp could be hashed into the public sync field (see below) to preclude packet-retry attacks.

[00137] In one embodiment, a "sync field" is added to the header of each packet sent out by the sender. This sync field could appear in the clear or as part of an encrypted portion of the packet. Assuming that a sender and receiver have selected a random-number generator (RNG) and seed value, this combination of RNG and seed can be used to generate a random-

Petitioner Apple Inc. - Exhibit 1002, p. 46

number sequence (RNS). The RNS is then used to generate a sequence of source/destination IP pairs (and, if desired, discriminator fields and hardware source and destination addresses), as described above. It is not necessary, however, to generate the entire sequence (or the first N-1 values) in order to generate the Nth random number in the sequence; if the sequence index N is known, the random value corresponding to that index can be directly generated (see below). Different RNGs (and seeds) with different fundamental periods could be used to generate the source and destination IP sequences, but the basic concepts would still apply. For the sake of simplicity, the following discussion will assume that IP source and destination address pairs (only) are hopped using a single RNG sequencing mechanism.

[00138] In accordance with a "self-synchronization" feature, a sync field in each packet header provides an index (i.e., a sequence number) into the RNS that is being used to generate IP pairs. Plugging this index into the RNG that is being used to generate the RNS yields a specific random number value, which in turn yields a specific IP pair. That is, an IP pair can be generated directly from knowledge of the RNG, seed, and index number; it is not necessary, in this scheme, to generate the entire sequence of random numbers that precede the sequence value associated with the index number provided.

[00139] Since the communicants have presumably previously exchanged RNGs and seeds, the only new information that must be provided in order to generate an IP pair is the sequence number. If this number is provided by the sender in the packet header, then the receiver need only plug this number into the RNG in order to generate an IP pair — and thus verify that the IP pair appearing in the header of the packet is valid. In this scheme, if the sender and receiver lose synchronization, the receiver can immediately re-synchronize upon receipt of a single packet by simply comparing the IP pair in the packet header to the IP pair generated from the index number. Thus, synchronized communications can be resumed upon receipt of a single packet, making this scheme ideal for multicast communications. Taken to the extreme, it could obviate the need for synchronization tables entirely; that is, the sender and receiver could simply rely on the index number in the sync field to validate the IP pair on each packet, and thereby eliminate the tables entirely.

[00140] The aforementioned scheme may have some inherent security issues associated with it — namely, the placement of the sync field. If the field is placed in the outer header, then an interloper could observe the values of the field and their relationship to the IP stream. This could potentially compromise the algorithm that is being used to generate the IP-address sequence, which would compromise the security of the communications. If, however, the value is placed in the inner header, then the sender must decrypt the inner header before it can extract the sync value and validate the IP pair; this opens up the receiver to certain types of denial-of-service (DoS) attacks, such as packet replay. That is, if the receiver must decrypt a packet before it can validate the IP pair, then it could potentially be forced to expend a significant amount of processing on decryption if an attacker simply retransmits previously valid packets. Other attack methodologies are possible in this scenario.

[00141] A possible compromise between algorithm security and processing speed is to split up the sync value between an inner (encrypted) and outer (unencrypted) header. That is, if the sync value is sufficiently long, it could potentially be split into a rapidly-changing part that can be viewed in the clear, and a fixed (or very slowly changing) part that must be protected. The part that can be viewed in the clear will be called the "public sync" portion and the part that must be protected will be called the "private sync" portion.

[00142] Both the public sync and private sync portions are needed to generate the complete sync value. The private portion, however, can be selected such that it is fixed or will change only occasionally. Thus, the private sync value can be stored by the recipient, thereby obviating the need to decrypt the header in order to retrieve it. If the sender and receiver have previously agreed upon the frequency with which the private part of the sync will change, then the receiver can selectively decrypt a single header in order to extract the new private sync if the communications gap that has led to lost synchronization has exceeded the lifetime of the previous private sync. This should not represent a burdensome amount of decryption, and thus should not open up the receiver to denial-of-service attack simply based on the need to occasionally decrypt a single header.

[00143] One implementation of this is to use a hashing function with a one-to-one mapping to generate the private and public sync portions from the sync value. This

implementation is shown in FIG. 13, where (for example) a first ISP 1302 is the sender and a second ISP 1303 is the receiver. (Other alternatives are possible from FIG. 13.) A transmitted packet comprises a public or "outer" header 1305 that is not encrypted, and a private or "inner" header 1306 that is encrypted using for example a link key. Outer header 1305 includes a public sync portion while inner header 1306 contains the private sync portion. A receiving node decrypts the inner header using a decryption function 1307 in order to extract the private sync portion. This step is necessary only if the lifetime of the currently buffered private sync has expired. (If the currently-buffered private sync is still valid, then it is simply extracted from memory and "added" (which could be an inverse hash) to the public sync, as shown in step 1308.) The public and decrypted private sync portions are combined in function 1308 in order to generate the combined sync 1309. The combined sync (1309) is then fed into the RNG (1310) and compared to the IP address pair (1311) to validate or reject the packet.

[00144] An important consideration in this architecture is the concept of "future" and "past" where the public sync values are concerned. Though the sync values, themselves, should be random to prevent spoofing attacks, it may be important that the receiver be able to quickly identify a sync value that has already been sent — even if the packet containing that sync value was never actually received by the receiver. One solution is to hash a time stamp or sequence number into the public sync portion, which could be quickly extracted, checked, and discarded, thereby validating the public sync portion itself.

[00145] In one embodiment, packets can be checked by comparing the source/destination IP pair generated by the sync field with the pair appearing in the packet header. If (1) they match, (2) the time stamp is valid, and (3) the dead-man timer has expired, then re-synchronization occurs; otherwise, the packet is rejected. If enough processing power is available, the dead-man timer and synchronization tables can be avoided altogether, and the receiver would simply resynchronize (e.g., validate) on every packet.

[00146] The foregoing scheme may require large-integer (e.g., 160-bit) math, which may affect its implementation. Without such large-integer registers, processing throughput would be affected, thus potentially affecting security from a denial-of-service standpoint. Nevertheless,

Petitioner Apple Inc. - Exhibit 1002, p. 49

as large integer math processing features become more prevalent, the costs of implementing such a feature will be reduced.

D. Other Synchronization Schemes

[00147] As explained above, if W or more consecutive packets are lost between a transmitter and receiver in a VPN (where W is the window size), the receiver's window will not have been updated and the transmitter will be transmitting packets not in the receiver's window. The sender and receiver will not recover synchronization until perhaps the random pairs in the window are repeated by chance. Therefore, there is a need to keep a transmitter and receiver in synchronization whenever possible and to re-establish synchronization whenever it is lost.

[00148] A "checkpoint" scheme can be used to regain synchronization between a sender and a receiver that have fallen out of synchronization. In this scheme, a checkpoint message comprising a random IP address pair is used for communicating synchronization information. In one embodiment, two messages are used to communicate synchronization information between a sender and a recipient:

1. SYNC_REQ is a message used by the sender to indicate that it wants to synchronize; and

2. SYNC_ACK is a message used by the receiver to inform the transmitter that it has been synchronized.

[00149] According to one variation of this approach, both the transmitter and receiver maintain three checkpoints (see FIG. 14):

1. In the transmitter, ckpt_o ("checkpoint old") is the IP pair that was used to re-send the last SYNC_REQ packet to the receiver. In the receiver, ckpt_o ("checkpoint old") is the IP pair that receives repeated SYNC_REQ packets from the transmitter.

2. In the transmitter, ckpt_n ("checkpoint new") is the IP pair that will be used to send the next SYNC_REQ packet to the receiver. In the receiver, ckpt_n ("checkpoint new") is the IP pair that receives a new SYNC_REQ packet from the transmitter and which causes the

receiver's window to be re-aligned, ckpt_o set to ckpt_n, a new ckpt_n to be generated and a new ckpt_r to be generated.

3. In the transmitter, ckpt_r is the IP pair that will be used to send the next SYNC_ACK packet to the receiver. In the receiver, ckpt_r is the IP pair that receives a new SYNC_ACK packet from the transmitter and which causes a new ckpt_n to be generated. Since SYNC_ACK is transmitted from the receiver ISP to the sender ISP, the transmitter ckpt_r refers to the ckpt_r of the receiver and the receiver ckpt_r refers to the ckpt_r of the transmitter (see FIG. 14).

When a transmitter initiates synchronization, the IP pair it will use to transmit the next data packet is set to a predetermined value and when a receiver first receives a SYNC_REQ, the receiver window is updated to be centered on the transmitter's next IP pair. This is the primary mechanism for checkpoint synchronization.

[00150] Synchronization can be initiated by a packet counter (e.g., after every N packets transmitted, initiate a synchronization) or by a timer (every S seconds, initiate a synchronization) or a combination of both. See FIG. 15. From the transmitter's perspective, this technique operates as follows: (1) Each transmitter periodically transmits a "sync request" message to the receiver to make sure that it is in sync. (2) If the receiver is still in sync, it sends back a "sync ack" message. (If this works, no further action is necessary). (3) If no "sync ack" has been received within a period of time, the transmitter retransmits the sync request again. If the transmitter reaches the next checkpoint without receiving a "sync ack" response, then synchronization is broken, and the transmitter should stop transmitting. The transmitter will continue to send sync_reqs until it receives a sync_ack, at which point transmission is reestablished.

[00151] From the receiver's perspective, the scheme operates as follows: (1) when it receives a "sync request" request from the transmitter, it advances its window to the next checkpoint position (even skipping pairs if necessary), and sends a "sync ack" message to the transmitter. If sync was never lost, then the "jump ahead" really just advances to the next available pair of addresses in the table (i.e., normal advancement).

[00152] If an interloper intercepts the "sync request" messages and tries to interfere with communication by sending new ones, it will be ignored if the synchronization has been established or it will actually help to re-establish synchronization.

[00153] A window is realigned whenever a re-synchronization occurs. This realignment entails updating the receiver's window to straddle the address pairs used by the packet transmitted immediately after the transmission of the SYNC_REQ packet. Normally, the transmitter and receiver are in synchronization with one another. However, when network events occur, the receiver's window may have to be advanced by many steps during resynchronization. In this case, it is desirable to move the window ahead without having to step through the intervening random numbers sequentially. (This feature is also desirable for the auto-sync approach discussed above).

E. Random Number Generator with a Jump-Ahead capability

[00154] An attractive method for generating randomly hopped addresses is to use identical random number generators in the transmitter and receiver and advance them as packets are transmitted and received. There are many random number generation algorithms that could be used. Each one has strengths and weaknesses for address hopping applications.

[00155] Linear congruential random number generators (LCRs) are fast, simple and well characterized random number generators that can be made to jump ahead *n* steps efficiently. An LCR generates random numbers X_1, X_2, X_3 ... Xk starting with seed X_0 using a recurrence

$$X_i=(a\ X_{i-1} + b) \bmod c, \qquad (1)$$

where a, b and c define a particular LCR. Another expression for X_i,

$$X_i=((a^i(X_0+b)-b)/(a-1)) \bmod c \qquad (2)$$

enables the jump-ahead capability. The factor a^i can grow very large even for modest i if left unfettered. Therefore some special properties of the modulo operation can be used to control the size and processing time required to compute (2). (2) can be rewritten as:

$$X_i=(a^i(X_0(a-1)+b)-b)/(a-1) \bmod c. \quad (3)$$

It can be shown that:

$$(a^i(X_0(a-1)+b)-b)/(a-1) \bmod c =$$

$$((a^i \bmod((a-1)c)(X_0(a-1)+b) -b) /(a-1)) \bmod c \quad (4).$$

[00156] $(X_0(a-1)+b)$ can be stored as $(X_0(a-1)+b) \bmod c$, b as b mod c and compute $a^i \bmod((a-1)c)$ (this requires O(log(i)) steps).

[00157] A practical implementation of this algorithm would jump a fixed distance, n, between synchronizations; this is tantamount to synchronizing every *n* packets. The window would commence *n* IP pairs from the start of the previous window. Using X_j^w, the random number at the jth checkpoint, as X_0 and *n* as *i*, a node can store $a^n \bmod((a- 1)c)$ once per LCR and set

[00158] $$X_{j+1}^w=X_{n(j+1)}=((a^n \bmod((a-1)c) (X_j^w (a-1)+b)-b)/(a-1))\bmod c, \quad (5)$$

to generate the random number for the $j+1^{th}$ synchronization. Using this construction, a node could jump ahead an arbitrary (but fixed) distance between synchronizations in a constant amount of time (independent of n).

[00159] Pseudo-random number generators, in general, and LCRs, in particular, will eventually repeat their cycles. This repetition may present vulnerability in the IP hopping scheme. An adversary would simply have to wait for a repeat to predict future sequences. One way of coping with this vulnerability is to create a random number generator with a known long cycle. A random sequence can be replaced by a new random number generator before it repeats. LCRs can be constructed with known long cycles. This is not currently true of many random number generators.

[00160] Random number generators can be cryptographically insecure. An adversary can derive the RNG parameters by examining the output or part of the output. This is true of

Petitioner Apple Inc. - Exhibit 1002, p. 53

LCGs. This vulnerability can be mitigated by incorporating an encryptor, designed to scramble the output as part of the random number generator. The random number generator prevents an adversary from mounting an attack—e.g., a known plaintext attack—against the encryptor.

F. Random Number Generator Example

[00161] Consider a RNG where a=31,b=4 and c=15. For this case equation (1) becomes:

$X_i=(31\ X_{i-1} + 4) \bmod 15.$ (6)

If one sets $X_0=1$, equation (6) will produce the sequence 1, 5, 9, 13, 2, 6, 10, 14, 3, 7, 11, 0, 4, 8, 12. This sequence will repeat indefinitely. For a jump ahead of 3 numbers in this sequence $a^n= 31^3=29791$, $c*(a-1)=15*30=450$ and $a^n \bmod((a-1)c) = 31^3 \bmod(15*30)=29791 \bmod(450)=91$. Equation (5) becomes:

$((91\ (X_i30+4)-4)/30) \bmod 15$ (7).

Table 1 shows the jump ahead calculations from (7) . The calculations start at 5 and jump ahead 3.

TABLE 1

I	X_i	(X_i30+4)	$91\ (X_i30+4)-4$	$((91\ (X_i30+4)-4)/30$	X_{i+3}
1	5	154	14010	467	2
4	2	64	5820	194	14
7	14	424	38580	1286	11
10	11	334	30390	1013	8
13	8	244	22200	740	5

G. Fast Packet Filter

[00162] Address hopping VPNs must rapidly determine whether a packet has a valid header and thus requires further processing, or has an invalid header (a hostile packet) and should be immediately rejected. Such rapid determinations will be referred to as "fast packet filtering." This capability protects the VPN from attacks by an adversary who streams hostile packets at the receiver at a high rate of speed in the hope of saturating the receiver's processor (a so-called "denial of service" attack). Fast packet filtering is an important feature for implementing VPNs on shared media such as Ethernet.

[00163] Assuming that all participants in a VPN share an unassigned "A" block of addresses, one possibility is to use an experimental "A" block that will never be assigned to any machine that is not address hopping on the shared medium. "A" blocks have a 24 bits of address that can be hopped as opposed to the 8 bits in "C" blocks. In this case a hopblock will be the "A" block. The use of the experimental "A" block is a likely option on an Ethernet because:

1. The addresses have no validity outside of the Ethernet and will not be routed out to a valid outside destination by a gateway.

2. There are 2^{24} (~16 million) addresses that can be hopped within each "A" block. This yields >280 trillion possible address pairs making it very unlikely that an adversary would guess a valid address. It also provides acceptably low probability of collision between separate VPNs (all VPNs on a shared medium independently generate random address pairs from the same "A" block).

3. The packets will not be received by someone on the Ethernet who is not on a VPN (unless the machine is in promiscuous mode) minimizing impact on non-VPN computers.

[00164] The Ethernet example will be used to describe one implementation of fast packet filtering. The ideal algorithm would quickly examine a packet header, determine whether the packet is hostile, and reject any hostile packets or determine which active IP pair the packet header matches. The problem is a classical associative memory problem. A variety of techniques

have been developed to solve this problem (hashing, B—trees etc). Each of these approaches has its strengths and weaknesses. For instance, hash tables can be made to operate quite fast in a statistical sense, but can occasionally degenerate into a much slower algorithm. This slowness can persist for a period of time. Since there is a need to discard hostile packets quickly at all times, hashing would be unacceptable.

H. Presence Vector Algorithm

[00165] A presence vector is a bit vector of length 2^n that can be indexed by n-bit numbers (each ranging from 0 to 2^n -1). One can indicate the presence of k n-bit numbers (not necessarily unique), by setting the bits in the presence vector indexed by each number to 1. Otherwise, the bits in the presence vector are 0. An n-bit number, x, is one of the k numbers if and only if the xth bit of the presence vector is 1. A fast packet filter can be implemented by indexing the presence vector and looking for a 1, which will be referred to as the "test."

[00166] For example, suppose one wanted to represent the number 135 using a presence vector. The 135th bit of the vector would be set. Consequently, one could very quickly determine whether an address of 135 was valid by checking only one bit: the 135th bit. The presence vectors could be created in advance corresponding to the table entries for the IP addresses. In effect, the incoming addresses can be used as indices into a long vector, making comparisons very fast. As each RNG generates a new address, the presence vector is updated to reflect the information. As the window moves, the presence vector is updated to zero out addresses that are no longer valid.

[00167] There is a trade-off between efficiency of the test and the amount of memory required for storing the presence vector(s). For instance, if one were to use the 48 bits of hopping addresses as an index, the presence vector would have to be 35 terabytes. Clearly, this is too large for practical purposes. Instead, the 48 bits can be divided into several smaller fields. For instance, one could subdivide the 48 bits into four 12-bit fields (see FIG. 16). This reduces the storage requirement to 2048 bytes at the expense of occasionally having to process a hostile packet. In effect, instead of one long presence vector, the decomposed address portions must match all four shorter presence vectors before further processing is allowed. (If the first part of

Petitioner Apple Inc. - Exhibit 1002, p. 56

the address portion doesn't match the first presence vector, there is no need to check the remaining three presence vectors).

[00168] A presence vector will have a 1 in the yth bit if and only if one or more addresses with a corresponding field of y are active. An address is active only if each presence vector indexed by the appropriate sub-field of the address is 1.

[00169] Consider a window of 32 active addresses and 3 checkpoints. A hostile packet will be rejected by the indexing of one presence vector more than 99% of the time. A hostile packet will be rejected by the indexing of all 4 presence vectors more than 99.9999995% of the time. On average, hostile packets will be rejected in less than 1.02 presence vector index operations.

[00170] The small percentage of hostile packets that pass the fast packet filter will be rejected when matching pairs are not found in the active window or are active checkpoints. Hostile packets that serendipitously match a header will be rejected when the VPN software attempts to decrypt the header. However, these cases will be extremely rare. There are many other ways this method can be configured to arbitrate the space/speed tradeoffs.

I. Further Synchronization Enhancements

[00171] A slightly modified form of the synchronization techniques described above can be employed. The basic principles of the previously described checkpoint synchronization scheme remain unchanged. The actions resulting from the reception of the checkpoints are, however, slightly different. In this variation, the receiver will maintain between OoO ("Out of Order") and 2xWINDOW_SIZE+OoO active addresses ($1 \leq OoO \leq WINDOW\_SIZE$ and $WINDOW\_SIZE \geq 1$). OoO and WINDOW_SIZE are engineerable parameters, where OoO is the minimum number of addresses needed to accommodate lost packets due to events in the network or out of order arrivals and WINDOW_SIZE is the number of packets transmitted before a SYNC_REQ is issued. FIG. 17 depicts a storage array for a receiver's active addresses.

[00172] The receiver starts with the first 2xWINDOW_SIZE addresses loaded and active (ready to receive data). As packets are received, the corresponding entries are marked as

"used" and are no longer eligible to receive packets. The transmitter maintains a packet counter, initially set to 0, containing the number of data packets transmitted since the last *initial* transmission of a SYNC_REQ for which SYNC_ACK has been received. When the transmitter packet counter equals WINDOW_SIZE, the transmitter generates a SYNC_REQ and does its initial transmission. When the receiver receives a SYNC_REQ corresponding to its current CKPT_N, it generates the next WINDOW_SIZE addresses and starts loading them in order starting at the first location after the last active address wrapping around to the beginning of the array after the end of the array has been reached. The receiver's array might look like FIG. 18 when a SYNC_REQ has been received. In this case a couple of packets have been either lost or will be received out of order when the SYNC_REQ is received.

[00173] FIG. 19 shows the receiver's array after the new addresses have been generated. If the transmitter does not receive a SYNC_ACK, it will re-issue the SYNC_REQ at regular intervals. When the transmitter receives a SYNC_ACK, the packet counter is decremented by WINDOW_SIZE. If the packet counter reaches 2xWINDOW_SIZE — OoO then the transmitter ceases sending data packets until the appropriate SYNC_ACK is finally received. The transmitter then resumes sending data packets. Future behavior is essentially a repetition of this initial cycle. The advantages of this approach are:

1. There is no need for an efficient jump ahead in the random number generator,

2. No packet is ever transmitted that does not have a corresponding entry in the receiver side

3. No timer based re-synchronization is necessary. This is a consequence of 2.

4. The receiver will always have the ability to accept data messages transmitted within OoO messages of the most recently transmitted message.

J. Distributed Transmission Path Variant

[00174] Another embodiment incorporating various inventive principles is shown in FIG. 20. In this embodiment, a message transmission system includes a first computer 2001 in communication with a second computer 2002 through a network 2011 of intermediary

Petitioner Apple Inc. - Exhibit 1002, p. 58

computers. In one variant of this embodiment, the network includes two edge routers 2003 and 2004 each of which is linked to a plurality of Internet Service Providers (ISPs) 2005 through 2010. Each ISP is coupled to a plurality of other ISPs in an arrangement as shown in FIG. 20, which is a representative configuration only and is not intended to be limiting. Each connection between ISPs is labeled in FIG. 20 to indicate a specific physical transmission path (e.g., AD is a physical path that links ISP A (element 2005) to ISP D (element 2008)). Packets arriving at each edge router are selectively transmitted to one of the ISPs to which the router is attached on the basis of a randomly or quasi-randomly selected basis.

[00175] As shown in FIG. 21, computer 2001 or edge router 2003 incorporates a plurality of link transmission tables 2100 that identify, for each potential transmission path through the network, valid sets of IP addresses that can be used to transmit the packet. For example, AD table 2101 contains a plurality of IP source/destination pairs that are randomly or quasi-randomly generated. When a packet is to be transmitted from first computer 2001 to second computer 2002, one of the link tables is randomly (or quasi-randomly) selected, and the next valid source/destination address pair from that table is used to transmit the packet through the network. If path AD is randomly selected, for example, the next source/destination IP address pair (which is pre-determined to transmit between ISP A (element 2005) and ISP B (element 2008)) is used to transmit the packet. If one of the transmission paths becomes degraded or inoperative, that link table can be set to a "down" condition as shown in table 2105, thus preventing addresses from being selected from that table. Other transmission paths would be unaffected by this broken link.

3. CONTINUATION-IN-PART IMPROVEMENTS

[00176] The following describes various improvements and features that can be applied to the embodiments described above. The improvements include: (1) a load balancer that distributes packets across different transmission paths according to transmission path quality; (2) a DNS proxy server that transparently creates a virtual private network in response to a domain name inquiry; (3) a large-to-small link bandwidth management feature that prevents denial-of-service attacks at system chokepoints; (4) a traffic limiter that regulates incoming packets by limiting the rate at which a transmitter can be synchronized with a receiver; and (5) a signaling

Petitioner Apple Inc. - Exhibit 1002, p. 59

synchronizer that allows a large number of nodes to communicate with a central node by partitioning the communication function between two separate entities. Each is discussed separately below.

A. Load Balancer

[00177] Various embodiments described above include a system in which a transmitting node and a receiving node are coupled through a plurality of transmission paths, and wherein successive packets are distributed quasi-randomly over the plurality of paths. See, for example, FIGS. 20 and 21 and accompanying description. The improvement extends this basic concept to encompass distributing packets across different paths in such a manner that the loads on the paths are generally balanced according to transmission link quality.

[00178] In one embodiment, a system includes a transmitting node and a receiving node that are linked via a plurality of transmission paths having potentially varying transmission quality. Successive packets are transmitted over the paths based on a weight value distribution function for each path. The rate that packets will be transmitted over a given path can be different for each path. The relative "health" of each transmission path is monitored in order to identify paths that have become degraded. In one embodiment, the health of each path is monitored in the transmitter by comparing the number of packets transmitted to the number of packet acknowledgements received. Each transmission path may comprise a physically separate path (e.g., via dial-up phone line, computer network, router, bridge, or the like), or may comprise logically separate paths contained within a broadband communication medium (e.g., separate channels in an FDM, TDM, CDMA, or other type of modulated or unmodulated transmission link).

[00179] When the transmission quality of a path falls below a predetermined threshold and there are other paths that can transmit packets, the transmitter changes the weight value used for that path, making it less likely that a given packet will be transmitted over that path. The weight will preferably be set no lower than a minimum value that keeps nominal traffic on the path. The weights of the other available paths are altered to compensate for the change in the affected path. When the quality of a path degrades to where the transmitter is turned off by the

Petitioner Apple Inc. - Exhibit 1002, p. 60

synchronization function (i.e., no packets are arriving at the destination), the weight is set to zero. If all transmitters are turned off, no packets are sent.

[00180] Conventional TCP/IP protocols include a "throttling" feature that reduces the transmission rate of packets when it is determined that delays or errors are occurring in transmission. In this respect, timers are sometimes used to determine whether packets have been received. These conventional techniques for limiting transmission of packets, however, do not involve multiple transmission paths between two nodes wherein transmission across a particular path relative to the others is changed based on link quality.

[00181] According to certain embodiments, in order to damp oscillations that might otherwise occur if weight distributions are changed drastically (e.g., according to a step function), a linear or an exponential decay formula can be applied to gradually decrease the weight value over time that a degrading path will be used. Similarly, if the health of a degraded path improves, the weight value for that path is gradually increased.

[00182] Transmission link health can be evaluated by comparing the number of packets that are acknowledged within the transmission window (see embodiments discussed above) to the number of packets transmitted within that window and by the state of the transmitter (i.e., on or off). In other words, rather than accumulating general transmission statistics over time for a path, one specific implementation uses the "windowing" concepts described above to evaluate transmission path health.

[00183] The same scheme can be used to shift virtual circuit paths from an "unhealthy" path to a "healthy" one, and to select a path for a new virtual circuit.

[00184] FIG. 22A shows a flowchart for adjusting weight values associated with a plurality of transmission links. It is assumed that software executing in one or more computer nodes executes the steps shown in FIG. 22A. It is also assumed that the software can be stored on a computer-readable medium such as a magnetic or optical disk for execution by a computer.

[00185] Beginning in step 2201, the transmission quality of a given transmission path is measured. As described above, this measurement can be based on a comparison between the

Petitioner Apple Inc. - Exhibit 1002, p. 61

number of packets transmitted over a particular link to the number of packet acknowledgements received over the link (e.g., per unit time, or in absolute terms). Alternatively, the quality can be evaluated by comparing the number of packets that are acknowledged within the transmission window to the number of packets that were transmitted within that window. In yet another variation, the number of missed synchronization messages can be used to indicate link quality. Many other variations are of course possible.

[00186] In step 2202, a check is made to determine whether more than one transmitter (e.g., transmission path) is turned on. If not, the process is terminated and resumes at step 2201.

[00187] In step 2203, the link quality is compared to a given threshold (e.g., 50%, or any arbitrary number). If the quality falls below the threshold, then in step 2207 a check is made to determine whether the weight is above a minimum level (e.g., 1%). If not, then in step 2209 the weight is set to the minimum level and processing resumes at step 2201. If the weight is above the minimum level, then in step 2208 the weight is gradually decreased for the path, then in step 2206 the weights for the remaining paths are adjusted accordingly to compensate (e.g., they are increased).

[00188] If in step 2203 the quality of the path was greater than or equal to the threshold, then in step 2204 a check is made to determine whether the weight is less than a steady-state value for that path. If so, then in step 2205 the weight is increased toward the steady-state value, and in step 2206 the weights for the remaining paths are adjusted accordingly to compensate (e.g., they are decreased). If in step 2204 the weight is not less than the steady-state value, then processing resumes at step 2201 without adjusting the weights.

[00189] The weights can be adjusted incrementally according to various functions, preferably by changing the value gradually. In one embodiment, a linearly decreasing function is used to adjust the weights; according to another embodiment, an exponential decay function is used. Gradually changing the weights helps to damp oscillators that might otherwise occur if the probabilities were abruptly.

Petitioner Apple Inc. - Exhibit 1002, p. 62

[00190] Although not explicitly shown in FIG. 22A the process can be performed only periodically (e.g., according to a time schedule), or it can be continuously run, such as in a background mode of operation. In one embodiment, the combined weights of all potential paths should add up to unity (e.g., when the weighting for one path is decreased, the corresponding weights that the other paths will be selected will increase).

[00191] Adjustments to weight values for other paths can be prorated. For example, a decrease of 10% in weight value for one path could result in an evenly distributed increase in the weights for the remaining paths. Alternatively, weightings could be adjusted according to a weighted formula as desired (e.g., favoring healthy paths over less healthy paths). In yet another variation, the difference in weight value can be amortized over the remaining links in a manner that is proportional to their traffic weighting.

[00192] FIG. 22B shows steps that can be executed to shut down transmission links where a transmitter turns off. In step 2210, a transmitter shut-down event occurs. In step 2211, a test is made to determine whether at least one transmitter is still turned on. If not, then in step 2215 all packets are dropped until a transmitter turns on. If in step 2211 at least one transmitter is turned on, then in step 2212 the weight for the path is set to zero, and the weights for the remaining paths are adjusted accordingly.

[00193] FIG. 23 shows a computer node 2301 employing various principles of the above- described embodiments. It is assumed that two computer nodes of the type shown in FIG. 23 communicate over a plurality of separate physical transmission paths. As shown in FIG. 23, four transmission paths X1 through X4 are defined for communicating between the two nodes. Each node includes a packet transmitter 2302 that operates in accordance with a transmit table 2308 as described above. (The packet transmitter could also operate without using the IP-hopping features described above, but the following description assumes that some form of hopping is employed in conjunction with the path selection mechanism.). The computer node also includes a packet receiver 2303 that operates in accordance with a receive table 2309, including a moving window W that moves as valid packets are received. Invalid packets having source and destination addresses that do not fall within window W are rejected.

Petitioner Apple Inc. - Exhibit 1002, p. 63

[00194] As each packet is readied for transmission, source and destination IP addresses (or other discriminator values) are selected from transmit table 2308 according to any of the various algorithms described above, and packets containing these source/destination address pairs, which correspond to the node to which the four transmission paths are linked, are generated to a transmission path switch 2307. Switch 2307, which can comprise a software function, selects from one of the available transmission paths according to a weight distribution table 2306. For example, if the weight for path X1 is 0.2, then every fifth packet will be transmitted on path Xl. A similar regime holds true for the other paths as shown. Initially, each link's weight value can be set such that it is proportional to its bandwidth, which will be referred to as its "steady-state" value.

[00195] Packet receiver 2303 generates an output to a link quality measurement function 2304 that operates as described above to determine the quality of each transmission path. (The input to packet receiver 2303 for receiving incoming packets is omitted for clarity). Link quality measurement function 2304 compares the link quality to a threshold for each transmission link and, if necessary, generates an output to weight adjustment function 2305. If a weight adjustment is required, then the weights in table 2306 are adjusted accordingly, preferably according to a gradual (e.g., linearly or exponentially declining) function. In one embodiment, the weight values for all available paths are initially set to the same value, and only when paths degrade in quality are the weights changed to reflect differences.

[00196] Link quality measurement function 2304 can be made to operate as part of a synchronizer function as described above. That is, if resynchronization occurs and the receiver detects that synchronization has been lost (e.g., resulting in the synchronization window W being advanced out of sequence), that fact can be used to drive link quality measurement function 2304. According to one embodiment, load balancing is performed using information garnered during the normal synchronization, augmented slightly to communicate link health from the receiver to the transmitter. The receiver maintains a count, MESS_R(W), of the messages received in synchronization window W. When it receives a synchronization request (SYNC_REQ) corresponding to the end of window W, the receiver includes counter MESS_R in the resulting synchronization acknowledgement (SYNC_ACK) sent back to the transmitter. This

Petitioner Apple Inc. - Exhibit 1002, p. 64

allows the transmitter to compare messages sent to messages received in order to asses the health of the link.

[00197] If synchronization is completely lost, weight adjustment function 2305 decreases the weight value on the affected path to zero. When synchronization is regained, the weight value for the affected path is gradually increased to its original value. Alternatively, link quality can be measured by evaluating the length of time required for the receiver to acknowledge a synchronization request. In one embodiment, separate transmit and receive tables are used for each transmission path.

[00198] When the transmitter receives a SYNC_ACK, the MESS_R is compared with the number of messages transmitted in a window (MESS_T). When the transmitter receives a SYNC_ACK, the traffic probabilities will be examined and adjusted if necessary. MESS_R is compared with the number of messages transmitted in a window (MESS_T). There are two possibilities:

1. If MESS_R is less than a threshold value, THRESH, then the link will be deemed to be unhealthy. If the transmitter was turned off, the transmitter is turned on and the weight P for that link will be set to a minimum value MIN. This will keep a trickle of traffic on the link for monitoring purposes until it recovers. If the transmitter was turned on, the weight P for that link will be set to:

$$P' = \alpha x\ MIN + (1 - \alpha) x P \quad (1)$$

Equation 1 will exponentially damp the traffic weight value to MIN during sustained periods of degraded service.

2. If MESS_R for a link is greater than or equal to THRESH, the link will be deemed healthy. If the weight P for that link is greater than or equal to the steady state value S for that link, then P is left unaltered. If the weight P for that link is less than THRESH then P will be set to:

$$P' = \beta x\ S + (1 - \beta) x P \quad (2)$$

where β is a parameter such that $0<=\beta<=1$ that determines the damping rate of P.

[00199] Equation 2 will increase the traffic weight to S during sustained periods of acceptable service in a damped exponential fashion.

[00200] A detailed example will now be provided with reference to FIG. 24. As shown in FIG. 24, a first computer 2401 communicates with a second computer 2402 through two routers 2403 and 2404. Each router is coupled to the other router through three transmission links. As described above, these may be physically diverse links or logical links (including virtual private networks).

[00201] Suppose that a first link L1 can sustain a transmission bandwidth of 100 Mb/s and has a window size of 32; link L2 can sustain 75 Mb/s and has a window size of 24; and link L3 can sustain 25 Mb/s and has a window size of 8. The combined links can thus sustain 200Mb/s. The steady state traffic weights are 0.5 for link L1; 0.375 for link L2, and 0.125 for link L3. MIN=1Mb/s, THRESH =0.8 MESS_T for each link, α=.75 and β=.5. These traffic weights will remain stable until a link stops for synchronization or reports a number of packets received less than its THRESH. Consider the following sequence of events:

1. Link L1 receives a SYNC_ACK containing a MESS_R of 24, indicating that only 75% of the MESS_T (32) messages transmitted in the last window were successfully received. Link 1 would be below THRESH (0.8). Consequently, link L1's traffic weight value would be reduced to 0.12825, while link L2's traffic weight value would be increased to 0.65812 and link L3's traffic weight value would be increased to 0.217938.

2. Link L2 and L3 remained healthy and link L1 stopped to synchronize. Then link L1's traffic weight value would be set to 0, link L2's traffic weight value would be set to 0.75, and link L33's traffic weight value would be set to 0.25.

3. Link L1 finally received a SYNC_ACK containing a MESS_R of 0 indicating that none of the MESS_T (32) messages transmitted in the last window were successfully received. Link L1 would be below THRESH. Link L1's traffic weight value would be increased to .005,

Petitioner Apple Inc. - Exhibit 1002, p. 66

link L2's traffic weight value would be decreased to 0.74625, and link L3's traffic weight value would be decreased to 0.24875.

4. Link Ll received a SYNC_ACK containing a MESS_R of 32 indicating that 100% of the MESS_T (32) messages transmitted in the last window were successfully received. Link L1 would be above THRESH. Link L1's traffic weight value would be increased to 0.2525, while link L2's traffic weight value would be decreased to 0.560625 and link L3's traffic weight value would be decreased to .186875.

5. Link L1 received a SYNC_ACK containing a MESS_R of 32 indicating that 100% of the MESS_T (32) messages transmitted in the last window were successfully received. Link L1 would be above THRESH. Link L1's traffic weight value would be increased to 0.37625; link L2's traffic weight value would be decreased to 0.4678125, and link L3's traffic weight value would be decreased to 0.1559375.

6. Link L1 remains healthy and the traffic probabilities approach their steady state traffic probabilities.

B. Use of a DNS Proxy to Transparently Create Virtual Private Networks

[00202] A second improvement concerns the automatic creation of a virtual private network (VPN) in response to a domain-name server look-up function.

[00203] Conventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host. For example, when a computer user types in the web name "Yahoo.com," the user's web browser transmits a request to a DNS, which converts the name into a four-part IP address that is returned to the user's browser and then used by the browser to contact the destination web site.

[00204] This conventional scheme is shown in FIG. 25. A user's computer 2501 includes a client application 2504 (for example, a web browser) and an IP protocol stack 2505. When the user enters the name of a destination host, a request DNS REQ is made (through IP protocol stack 2505) to a DNS 2502 to look up the IP address associated with the name. The DNS returns the IP address DNS RESP to client application 2504, which is then able to use the

IP address to communicate with the host 2503 through separate transactions such as PAGE REQ and PAGE RESP.

[00205] In the conventional architecture shown in FIG. 25, nefarious listeners on the Internet could intercept the DNS REQ and DNS RESP packets and thus learn what IP addresses the user was contacting. For example, if a user wanted to set up a secure communication path with a web site having the name "Target.com," when the user's browser contacted a DNS to find the IP address for that web site, the true IP address of that web site would be revealed over the Internet as part of the DNS inquiry. This would hamper anonymous communications on the Internet.

[00206] One conventional scheme that provides secure virtual private networks over the Internet provides the DNS server with the public keys of the machines that the DNS server has the addresses for. This allows hosts to retrieve automatically the public keys of a host that the host is to communicate with so that the host can set up a VPN without having the user enter the public key of the destination host. One implementation of this standard is presently being developed as part of the FreeS/WAN project(RFC 2535).

[00207] The conventional scheme suffers from certain drawbacks. For example, any user can perform a DNS request. Moreover, DNS requests resolve to the same value for all users.

[00208] According to certain aspects of the invention, a specialized DNS server traps DNS requests and, if the request is from a special type of user (e.g., one for which secure communication services are defined), the server does not return the true IP address of the target node, but instead automatically sets up a virtual private network between the target node and the user. The VPN is preferably implemented using the IP address "hopping" features of the basic invention described above, such that the true identity of the two nodes cannot be determined even if packets during the communication are intercepted. For DNS requests that are determined to not require secure services (e.g., an unregistered user), the DNS server transparently "passes through" the request to provide a normal look-up function and return the IP address of the target web server, provided that the requesting host has permissions to resolve unsecured sites. Different users who make an identical DNS request could be provided with different results.

Petitioner Apple Inc. - Exhibit 1002, p. 68

[00209] FIG. 26 shows a system employing various principles summarized above. A user's computer 2601 includes a conventional client (e.g., a web browser) 2605 and an IP protocol stack 2606 that preferably operates in accordance with an IP hopping function 2607 as outlined above. A modified DNS server 2602 includes a conventional DNS server function 2609 and a DNS proxy 2610. A gatekeeper server 2603 is interposed between the modified DNS server and a secure target site 2704. An "unsecure" target site 2611 is also accessible via conventional IP protocols.

[00210] According to one embodiment, DNS proxy 2610 intercepts all DNS lookup functions from client 2605 and determines whether access to a secure site has been requested. If access to a secure site has been requested (as determined, for example, by a domain name extension, or by reference to an internal table of such sites), DNS proxy 2610 determines whether the user has sufficient security privileges to access the site. If so, DNS proxy 2610 transmits a message to gatekeeper 2603 requesting that a virtual private network be created between user computer 2601 and secure target site 2604. In one embodiment, gatekeeper 2603 creates "hopblocks" to be used by computer 2601 and secure target site 2604 for secure communication. Then, gatekeeper 2603 communicates these to user computer 2601. Thereafter, DNS proxy 2610 returns to user computer 2601 the resolved address passed to it by the gatekeeper (this address could be different from the actual target computer) 2604, preferably using a secure administrative VPN. The address that is returned need not be the actual address of the destination computer.

[00211] Had the user requested lookup of a non-secure web site such as site 2611, DNS proxy would merely pass through to conventional DNS server 2609 the look-up request, which would be handled in a conventional manner, returning the IP address of non-secure web site 2611. If the user had requested lookup of a secure web site but lacked credentials to create such a connection, DNS proxy 2610 would return a "host unknown" error to the user. In this manner, different users requesting access to the same DNS name could be provided with different look-up results.

[00212] Gatekeeper 2603 can be implemented on a separate computer (as shown in FIG. 26) or as a function within modified DNS server 2602. In general, it is anticipated that

Petitioner Apple Inc. - Exhibit 1002, p. 69

gatekeeper 2703 facilitates the allocation and exchange of information needed to communicate securely, such as using "hopped" IP addresses. Secure hosts such as site 2604 are assumed to be equipped with a secure communication function such as an IP hopping function 2608.

[00213] It will be appreciated that the functions of DNS proxy 2610 and DNS server 2609 can be combined into a single server for convenience. Moreover, although element 2602 is shown as combining the functions of two servers, the two servers can be made to operate independently.

[00214] FIG. 27 shows steps that can be executed by DNS proxy server 2610 to handle requests for DNS look-up for secure hosts. In step 2701, a DNS look-up request is received for a target host. In step 2702, a check is made to determine whether access to a secure host was requested. If not, then in step 2703 the DNS request is passed to conventional DNS server 2609, which looks up the IP address of the target site and returns it to the user's application for further processing.

[00215] In step 2702, if access to a secure host was requested, then in step 2704 a further check is made to determine whether the user is authorized to connect to the secure host. Such a check can be made with reference to an internally stored list of authorized IP addresses, or can be made by communicating with gatekeeper 2603 (e.g., over an "administrative" VPN that is secure). It will be appreciated that different levels of security can also be provided for different categories of hosts. For example, some sites may be designated as having a certain security level, and the security level of the user requesting access must match that security level. The user's security level can also be determined by transmitting a request message back to the user's computer requiring that it prove that it has sufficient privileges.

[00216] If the user is not authorized to access the secure site, then a "host unknown" message is returned (step 2705). If the user has sufficient security privileges, then in step 2706 a secure VPN is established between the user's computer and the secure target site. As described above, this is preferably done by allocating a hopping regime that will be carried out between the user's computer and the secure target site, and is preferably performed transparently to the user (i.e., the user need not be involved in creating the secure link). As described in various

Petitioner Apple Inc. - Exhibit 1002, p. 70

embodiments of this application, any of various fields can be "hopped" (e.g., IP source/destination addresses; a field in the header; etc.) in order to communicate securely.

[00217] Some or all of the security functions can be embedded in gatekeeper 2603, such that it handles all requests to connect to secure sites. In this embodiment, DNS proxy 2610 communicates with gatekeeper 2603 to determine (preferably over a secure administrative VPN) whether the user has access to a particular web site. Various scenarios for implementing these features are described by way of example below:

[00218] Scenario #1: Client has permission to access target computer, and gatekeeper has a rule to make a VPN for the client. In this scenario, the client's DNS request would be received by the DNS proxy server 2610, which would forward the request to gatekeeper 2603. The gatekeeper would establish a VPN between the client and the requested target. The gatekeeper would provide the address of the destination to the DNS proxy, which would then return the resolved name as a result. The resolved address can be transmitted back to the client in a secure administrative VPN.

[00219] Scenario #2: Client does not have permission to access target computer. In this scenario, the client's DNS request would be received by the DNS proxy server 2610, which would forward the request to gatekeeper 2603. The gatekeeper would reject the request, informing DNS proxy server 2610 that it was unable to find the target computer. The DNS proxy 2610 would then return a "host unknown" error message to the client.

[00220] Scenario #3: Client has permission to connect using a normal non-VPN link, and the gatekeeper does not have a rule to set up a VPN for the client to the target site. In this scenario, the client's DNS request is received by DNS proxy server 2610, which would check its rules and determine that no VPN is needed. Gatekeeper 2603 would then inform the DNS proxy server to forward the request to conventional DNS server 2609, which would resolve the request and return the result to the DNS proxy server and then back to the client.

[00221] Scenario #4: Client does not have permission to establish a normal/non-VPN link, and the gatekeeper does not have a rule to make a VPN for the client to the target site. In

this scenario, the DNS proxy server would receive the client's DNS request and forward it to gatekeeper 2603. Gatekeeper 2603 would determine that no special VPN was needed, but that the client is not authorized to communicate with non-VPN members. The gatekeeper would reject the request, causing DNS proxy server 2610 to return an error message to the client.

C. Large Link to Small Link Bandwidth Management

[00222] One feature of the basic architecture is the ability to prevent so-called "denial of service" attacks that can occur if a computer hacker floods a known Internet node with packets, thus preventing the node from communicating with other nodes. Because IP addresses or other fields are "hopped" and packets arriving with invalid addresses are quickly discarded, Internet nodes are protected against flooding targeted at a single IP address.

[00223] In a system in which a computer is coupled through a link having a limited bandwidth (e.g., an edge router) to a node that can support a much higher-bandwidth link (e.g., an Internet Service Provider), a potential weakness could be exploited by a determined hacker. Referring to FIG. 28, suppose that a first host computer 2801 is communicating with a second host computer 2804 using the IP address hopping principles described above. The first host computer is coupled through an edge router 2802 to an Internet Service Provider (ISP) 2803 through a low bandwidth link (LOW BW), and is in turn coupled to second host computer 2804 through parts of the Internet through a high bandwidth link (HIGH BW). In this architecture, the ISP is able to support a high bandwidth to the internet, but a much lower bandwidth to the edge router 2802.

[00224] Suppose that a computer hacker is able to transmit a large quantity of dummy packets addressed to first host computer 2801 across high bandwidth link HIGH BW. Normally, host computer 2801 would be able to quickly reject the packets since they would not fall within the acceptance window permitted by the IP address hopping scheme. However, because the packets must travel across low bandwidth link LOW BW, the packets overwhelm the lower bandwidth link before they are received by host computer 2801. Consequently, the link to host computer 2801 is effectively flooded before the packets can be discarded.

[00225] According to one inventive improvement, a "link guard" function 2805 is inserted into the high-bandwidth node (e.g., ISP 2803) that quickly discards packets destined for a low- bandwidth target node if they are not valid packets. Each packet destined for a low-bandwidth node is cryptographically authenticated to determine whether it belongs to a VPN. If it is not a valid VPN packet, the packet is discarded at the high-bandwidth node. If the packet is authenticated as belonging to a VPN, the packet is passed with high preference. If the packet is a valid non-VPN packet, it is passed with a lower quality of service (e.g., lower priority).

[00226] In one embodiment, the ISP distinguishes between VPN and non-VPN packets using the protocol of the packet. In the case of IPSEC [rfc 2401], the packets have IP protocols 420 and 421. In the case of the TARP VPN, the packets will have an IP protocol that is not yet defined. The ISP's link guard, 2805, maintains a table of valid VPNs which it uses to validate whether VPN packets are cryptographically valid. According to one embodiment, packets that do not fall within any hop windows used by nodes on the low-bandwidth link are rejected, or are sent with a lower quality of service. One approach for doing this is to provide a copy of the IP hopping tables used by the low-bandwidth nodes to the high-bandwidth node, such that both the high-bandwidth and low-bandwidth nodes track hopped packets (e.g., the high-bandwidth node moves its hopping window as valid packets are received). In such a scenario, the high-bandwidth node discards packets that do not fall within the hopping window before they are transmitted over the low-bandwidth link. Thus, for example, ISP 2903 maintains a copy 2910 of the receive table used by host computer 2901. Incoming packets that do not fall within this receive table are discarded. According to a different embodiment, link guard 2805 validates each VPN packet using a keyed hashed message authentication code (HMAC) [rfc 2104].

[00227] According to another embodiment, separate VPNs (using, for example, hopblocks) can be established for communicating between the low-bandwidth node and the high-bandwidth node (i.e., packets arriving at the high-bandwidth node are converted into different packets before being transmitted to the low-bandwidth node).

[00228] As shown in FIG. 29, for example, suppose that a first host computer 2900 is communicating with a second host computer 2902 over the Internet, and the path includes a high

Petitioner Apple Inc. - Exhibit 1002, p. 73

bandwidth link HIGH BW to an ISP 2901 and a low bandwidth link LOW BW through an edge router 2904. In accordance with the basic architecture described above, first host computer 2900 and second host computer 2902 would exchange hopblocks (or a hopblock algorithm) and would be able to create matching transmit and receive tables 2905, 2906, 2912 and 2913. Then in accordance with the basic architecture, the two computers would transmit packets having seemingly random IP source and destination addresses, and each would move a corresponding hopping window in its receive table as valid packets were received.

[00229] Suppose that a nefarious computer hacker 2903 was able to deduce that packets having a certain range of IP addresses (e.g., addresses 100 to 200 for the sake of simplicity) are being transmitted to ISP 2901, and that these packets are being forwarded over a low-bandwidth link. Hacker computer 2903 could thus "flood" packets having addresses falling into the range 100 to 200, expecting that they would be forwarded along low bandwidth link LOW BW, thus causing the low bandwidth link to become overwhelmed. The fast packet reject mechanism in first host computer 3000 would be of little use in rejecting these packets, since the low bandwidth link was effectively jammed before the packets could be rejected. In accordance with one aspect of the improvement, however, VPN link guard 2911 would prevent the attack from impacting the performance of VPN traffic because the packets would either be rejected as invalid VPN packets or given a lower quality of service than VPN traffic over the lower bandwidth link. A denial-of- service flood attack could, however, still disrupt non-VPN traffic.

[00230] According to one embodiment of the improvement, ISP 2901 maintains a separate VPN with first host computer 2900, and thus translates packets arriving at the ISP into packets having a different IP header before they are transmitted to host computer 2900. The cryptographic keys used to authenticate VPN packets at the link guard 2911 and the cryptographic keys used to encrypt and decrypt the VPN packets at host 2902 and host 2901 can be different, so that link guard 2911 does not have access to the private host data; it only has the capability to authenticate those packets.

[00231] According to yet a third embodiment, the low-bandwidth node can transmit a special message to the high-bandwidth node instructing it to shut down all transmissions on a particular IP address, such that only hopped packets will pass through to the low-bandwidth

Petitioner Apple Inc. - Exhibit 1002, p. 74

node. This embodiment would prevent a hacker from flooding packets using a single IP address. According to yet a fourth embodiment, the high-bandwidth node can be configured to discard packets transmitted to the low-bandwidth node if the transmission rate exceeds a certain predetermined threshold for any given IP address; this would allow hopped packets to go through. In this respect, link guard 2911 can be used to detect that the rate of packets on a given IP address are exceeding a threshold rate; further packets addressed to that same IP address would be dropped or transmitted at a lower priority (e.g., delayed).

D. Traffic Limiter

[00232] In a system in which multiple nodes are communicating using "hopping" technology, a treasonous insider could internally flood the system with packets. In order to prevent this possibility, one inventive improvement involves setting up "contracts" between nodes in the system, such that a receiver can impose a bandwidth limitation on each packet sender. One technique for doing this is to delay acceptance of a checkpoint synchronization request from a sender until a certain time period (e.g., one minute) has elapsed. Each receiver can effectively control the rate at which its hopping window moves by delaying "SYNC_ACK" responses to "SYNC_REQ" messages.

[00233] A simple modification to the checkpoint synchronizer will serve to protect a receiver from accidental or deliberate overload from an internally treasonous client. This modification is based on the observation that a receiver will not update its tables until a SYNC_REQ is received on hopped address CKPT_N. It is a simple matter of deferring the generation of a new CKPT_N until an appropriate interval after previous checkpoints.

[00234] Suppose a receiver wished to restrict reception from a transmitter to 100 packets a second, and that checkpoint synchronization messages were triggered every 50 packets, A compliant transmitter would not issue new SYNC_REQ messages more often than every 0.5 seconds. The receiver could delay a non-compliant transmitter from synchronizing by delaying the issuance of CKPT_N for 0.5 second after the last SYNC_REQ was accepted.

[00235] In general, if M receivers need to restrict N transmitters issuing new SYNC_REQ messages after every W messages to sending R messages a second in aggregate,

each receiver could defer issuing a new CKPT_N until MxNxW/R seconds have elapsed since the last SYNC_REQ has been received and accepted. If the transmitter exceeds this rate between a pair of checkpoints, it will issue the new checkpoint before the receiver is ready to receive it, and the SYNC_REQ will be discarded by the receiver. After this, the transmitter will re-issue the SYNC_REQ every T1 seconds until it receives a SYNC_ACK. The receiver will eventually update CKPT_N and the SYNC_REQ will be acknowledged. If the transmission rate greatly exceeds the allowed rate, the transmitter will stop until it is compliant. If the transmitter exceeds the allowed rate by a little, it will eventually stop after several rounds of delayed synchronization until it is in compliance. Hacking the transmitter's code to not shut off only permits the transmitter to lose the acceptance window. In this case it can recover the window and proceed only after it is compliant again.

[00236] Two practical issues should be considered when implementing the above scheme:

1. The receiver rate should be slightly higher than the permitted rate in order to allow for statistical fluctuations in traffic arrival times and non-uniform load balancing.

2. Since a transmitter will rightfully continue to transmit for a period after a SYNC_REQ is transmitted, the algorithm above can artificially reduce the transmitter's bandwidth. If events prevent a compliant transmitter from synchronizing for a period (e.g. the network dropping a SYNC_REQ or a SYNC_ACK) a SYNC_REQ will be accepted later than expected. After this, the transmitter will transmit fewer than expected messages before encountering the next checkpoint. The new checkpoint will not have been activated and the transmitter will have to retransmit the SYNC_REQ. This will appear to the receiver as if the transmitter is not compliant. Therefore, the next checkpoint will be accepted late from the transmitter's perspective. This has the effect of reducing the transmitter's allowed packet rate until the transmitter transmits at a packet rate below the agreed upon rate for a period of time.

[00237] To guard against this, the receiver should keep track of the times that the last C SYNC_REQs were received and accepted and use the minimum of MxNxW/R seconds after the last SYNC_REQ has been received and accepted, 2xMxNxW/R seconds after next to the last

Petitioner Apple Inc. - Exhibit 1002, p. 76

SYNC_REQ has been received and accepted, CxMxNxW/R seconds after $(C-1)^{th}$ to the last SYNC_REQ has been received, as the time to activate CKPT_N. This prevents the receiver from inappropriately limiting the transmitter's packet rate if at least one out of the last C SYNC_REQs was processed on the first attempt.

[00238] FIG. 30 shows a system employing the above-described principles. In FIG. 30, two computers 3000 and 3001 are assumed to be communicating over a network N in accordance with the "hopping" principles described above (e.g., hopped IP addresses, discriminator values, etc.). For the sake of simplicity, computer 3000 will be referred to as the receiving computer and computer 3001 will be referred to as the transmitting computer, although full duplex operation is of course contemplated. Moreover, although only a single transmitter is shown, multiple transmitters can transmit to receiver 3000.

[00239] As described above, receiving computer 3000 maintains a receive table 3002 including a window W that defines valid IP address pairs that will be accepted when appearing in incoming data packets. Transmitting computer 3001 maintains a transmit table 3003 from which the next IP address pairs will be selected when transmitting a packet to receiving computer 3000. (For the sake of illustration, window W is also illustrated with reference to transmit table 3003). As transmitting computer moves through its table, it will eventually generate a SYNC_REQ message as illustrated in function 3010. This is a request to receiver 3000 to synchronize the receive table 3002, from which transmitter 3001 expects a response in the form of a CKPT_N (included as part of a SYNC_ACK message). If transmitting computer 3001 transmits more messages than its allotment, it will prematurely generate the SYNC_REQ message. (If it has been altered to remove the SYNC_REQ message generation altogether, it will fall out of synchronization since receiver 3000 will quickly reject packets that fall outside of window W, and the extra packets generated by transmitter 3001 will be discarded).

[00240] In accordance with the improvements described above, receiving computer 3000 performs certain steps when a SYNC_REQ message is received, as illustrated in FIG. 30. In step 3004, receiving computer 3000 receives the SYNC_REQ message. In step 3005, a check is made to determine whether the request is a duplicate. If so, it is discarded in step 3006. In step 3007, a check is made to determine whether the SYNC_REQ received from transmitter 3001 was

Petitioner Apple Inc. - Exhibit 1002, p. 77

received at a rate that exceeds the allowable rate R (i.e., the period between the time of the last SYNC_REQ message). The value R can be a constant, or it can be made to fluctuate as desired. If the rate exceeds R, then in step 3008 the next activation of the next CKPT_N hopping table entry is delayed by W/R seconds after the last SYNC_REQ has been accepted.

[00241] Otherwise, if the rate has not been exceeded, then in step 3109 the next CKPT_N value is calculated and inserted into the receiver's hopping table prior to the next SYNC_REQ from the transmitter 3101. Transmitter 3101 then processes the SYNC_REQ in the normal manner.

E. Signaling Synchronizer

[00242] In a system in which a large number of users communicate with a central node using secure hopping technology, a large amount of memory must be set aside for hopping tables and their supporting data structures. For example, if one million subscribers to a web site occasionally communicate with the web site, the site must maintain one million hopping tables, thus using up valuable computer resources, even though only a small percentage of the users may actually be using the system at any one time. A desirable solution would be a system that permits a certain maximum number of simultaneous links to be maintained, but which would "recognize" millions of registered users at any one time. In other words, out of a population of a million registered users, a few thousand at a time could simultaneously communicate with a central server, without requiring that the server maintain one million hopping tables of appreciable size.

[00243] One solution is to partition the central node into two nodes: a signaling server that performs session initiation for user log-on and log-off (and requires only minimally sized tables), and a transport server that contains larger hopping tables for the users. The signaling server listens for the millions of known users and performs a fast-packet reject of other (bogus) packets. When a packet is received from a known user, the signaling server activates a virtual private link (VPL) between the user and the transport server, where hopping tables are allocated and maintained. When the user logs onto the signaling server, the user's computer is provided with hop tables for communicating with the transport server, thus activating the VPL. The VPLs can be torn down when they become inactive for a time period, or they can be torn down upon

user log-out. Communication with the signaling server to allow user log-on and log-off can be accomplished using a specialized version of the checkpoint scheme described above.

[00244] FIG. 31 shows a system employing certain of the above-described principles. In FIG. 31, a signaling server 3101 and a transport server 3102 communicate over a link. Signaling server 3101 contains a large number of small tables 3106 and 3107 that contain enough information to authenticate a communication request with one or more clients 3103 and 3104. As described in more detail below, these small tables may advantageously be constructed as a special case of the synchronizing checkpoint tables described previously. Transport server 3102, which is preferably a separate computer in communication with signaling server 3101, contains a smaller number of larger hopping tables 3108, 3109, and 3110 that can be allocated to create a VPN with one of the client computers.

[00245] According to one embodiment, a client that has previously registered with the system (e.g., via a system administration function, a user registration procedure, or some other method) transmits a request for information from a computer (e.g., a web site). In one variation, the request is made using a "hopped" packet, such that signaling server 3101 will quickly reject invalid packets from unauthorized computers such as hacker computer 3105. An "administrative" VPN can be established between all of the clients and the signaling server in order to ensure that a hacker cannot flood signaling server 3101 with bogus packets. Details of this scheme are provided below.

[00246] Signaling server 3101 receives the request 3111 and uses it to determine that client 3103 is a validly registered user. Next, signaling server 3101 issues a request to transport server 3102 to allocate a hopping table (or hopping algorithm or other regime) for the purpose of creating a VPN with client 3103. The allocated hopping parameters are returned to signaling server 3101 (path 3113), which then supplies the hopping parameters to client 3103 via path 3114, preferably in encrypted form.

[00247] Thereafter, client 3103 communicates with transport server 3102 using the normal hopping techniques described above. It will be appreciated that although signaling server 3101 and transport server 3102 are illustrated as being two separate computers, they could of

Petitioner Apple Inc. - Exhibit 1002, p. 79

course be combined into a single computer and their functions performed on the single computer. Alternatively, it is possible to partition the functions shown in FIG. 31 differently from as shown without departing from the inventive principles.

[00248] One advantage of the above-described architecture is that signaling server 3101 need only maintain a small amount of information on a large number of potential users, yet it retains the capability of quickly rejecting packets from unauthorized users such as hacker computer 3105. Larger data tables needed to perform the hopping and synchronization functions are instead maintained in a transport server 3102, and a smaller number of these tables are needed since they are only allocated for "active" links. After a VPN has become inactive for a certain time period (e.g., one hour), the VPN can be automatically torn down by transport server 3102 or signaling server 3101.

[00249] A more detailed description will now be provided regarding how a special case of the checkpoint synchronization feature can be used to implement the signaling scheme described above.

[00250] The signaling synchronizer may be required to support many (millions) of standing, low bandwidth connections. It therefore should minimize per-VPL memory usage while providing the security offered by hopping technology. In order to reduce memory usage in the signaling server, the data hopping tables can be completely eliminated and data can be carried as part of the SYNC_REQ message. The table used by the server side (receiver) and client side (transmitter) is shown schematically as element 3106 in FIG. 31.

[00251] The meaning and behaviors of CKPT_N, CKPT_O and CKPT_R remain the same from the previous description, except that CKPT_N can receive a combined data and SYNC_REQ message or a SYNC_REQ message without the data.

[00252] The protocol is a straightforward extension of the earlier synchronizer. Assume that a client transmitter is on and the tables are synchronized. The initial tables can be generated "out of band." For example, a client can log into a web server to establish an account

Petitioner Apple Inc. - Exhibit 1002, p. 80

over the Internet. The client will receive keys etc encrypted over the Internet. Meanwhile, the server will set up the signaling VPN on the signaling server.

[00253] Assuming that a client application wishes to send a packet to the server on the client's standing signaling VPL:

1. The client sends the message marked as a data message on the inner header using the transmitter's CKPT_N address. It turns the transmitter off and starts a timer T1 noting CKPT_O. Messages can be one of three types: DATA, SYNC_REQ and SYNC_ACK. In the normal algorithm, some potential problems can be prevented by identifying each message type as part of the encrypted inner header field. In this algorithm, it is important to distinguish a data packet and a SYNC_REQ in the signaling synchronizer since the data and the SYNC_REQ come in on the same address.

2. When the server receives a data message on its CKPT_N, it verifies the message and passes it up the stack. The message can be verified by checking message type and other information (i.e., user credentials) contained in the inner header It replaces its CKPT_O with CKPT_N and generates the next CKPT_N. It updates its transmitter side CKPT_R to correspond to the client's receiver side CKPT_R and transmits a SYNC_ACK containing CKPT_O in its payload.

3. When the client side receiver receives a SYNC_ACK on its CKPT_R with a payload matching its transmitter side CKPT_O and the transmitter is off, the transmitter is turned on and the receiver side CKPT_R is updated. If the SYNC_ACK's payload does not match the transmitter side CKPT_O or the transmitter is on, the SYNC_ACK is simply discarded.

4. T1 expires: If the transmitter is off and the client's transmitter side CKPT_O matches the CKPTO associated with the timer, it starts timer T1 noting CKPT_O again, and a SYNC_REQ is sent using the transmitter's CKPT_O address. Otherwise, no action is taken.

5. When the server receives a SYNC_REQ on its CKPT_N, it replaces its CKPT_O with CKPT_N and generates the next CKPT_N. It updates its transmitter side CKPT_R to

Petitioner Apple Inc. - Exhibit 1002, p. 81

correspond to the client's receiver side CKPT_R and transmits a SYNC_ACK containing CKPT_O in its payload.

6. When the server receives a SYNC_REQ on its CKPT_O, it updates its transmitter side CKPT_R to correspond to the client's receiver side CKPT_R and transmits a SYNC_ACK containing CKPT_O in its payload.

[00254] FIG. 32 shows message flows to highlight the protocol. Reading from top to bottom, the client sends data to the server using its transmitter side CKPT_N. The client side transmitter is turned off and a retry timer is turned off. The transmitter will not transmit messages as long as the transmitter is turned off. The client side transmitter then loads CKPT_N into CKPT_O and updates CKPT_N. This message is successfully received and a passed up the stack. It also synchronizes the receiver i.e., the server loads CKPT_N into CKPT_O and generates a new CKPT_N, it generates a new CKPT_R in the server side transmitter and transmits a SYNC_ACK containing the server side receiver's CKPT_O the server. The SYNC_ACK is successfully received at the client. The client side receiver's CKPT_R is updated, the transmitter is turned on and the retry timer is killed. The client side transmitter is ready to transmit a new data message.

[00255] Next, the client sends data to the server using its transmitter side CKPT_N. The client side transmitter is turned off and a retry timer is turned off. The transmitter will not transmit messages as long as the transmitter is turned off. The client side transmitter then loads CKPT_N into CKPT_O and updates CKPT_N. This message is lost. The client side timer expires and as a result a SYNC_REQ is transmitted on the client side transmitter's CKPT_O (this will keep happening until the SYNC_ACK has been received at the client). The SYNC_REQ is successfully received at the server. It synchronizes the receiver i.e., the server loads CKPT_N into CKPT_O and generates a new CKPT_N, it generates an new CKPT_R in the server side transmitter and transmits a SYNC_ACK containing the server side receiver's CKPT_O the server. The SYNC_ACK is successfully received at the client. The client side receiver's CKPT_R is updated, the transmitter is turned off and the retry timer is killed. The client side transmitter is ready to transmit a new data message.

Petitioner Apple Inc. - Exhibit 1002, p. 82

[00256] There are numerous other scenarios that follow this flow. For example, the SYNC_ACK could be lost. The transmitter would continue to re-send the SYNC_REQ until the receiver synchronizes and responds.

[00257] The above-described procedures allow a client to be authenticated at signaling server 3201 while maintaining the ability of signaling server 3201 to quickly reject invalid packets, such as might be generated by hacker computer 3205. In various embodiments, the signaling synchronizer is really a derivative of the synchronizer. It provides the same protection as the hopping protocol, and it does so for a large number of low bandwidth connections.

F. One-Click Secure On-line Communications and Secure Domain Name Service

[00258] The present invention provides a technique for establishing a secure communication link between a first computer and a second computer over a computer network. Preferably, a user enables a secure communication link using a single click of a mouse, or a corresponding minimal input from another input device, such as a keystroke entered on a keyboard or a click entered through a trackball. Alternatively, the secure link is automatically established as a default setting at boot-up of the computer (i.e., no click). FIG. 33 shows a system block diagram 3300 of a computer network in which the one-click secure communication method of the present invention is suitable. In FIG. 33, a computer terminal or client computer 3301, such as a personal computer (PC), is connected to a computer network 3302, such as the Internet, through an ISP 3303. Alternatively, computer 3301 can be connected to computer network 3302 through an edge router. Computer 3301 includes an input device, such as a keyboard and/or mouse, and a display device, such as a monitor. Computer 3301 can communicate conventionally with another computer 3304 connected to computer network 3302 over a communication link 3305 using a browser 3306 that is installed and operates on computer 3301 in a well-known manner.

[00259] Computer 3304 can be, for example, a server computer that is used for conducting e-commerce. In the situation when computer network 3302 is the Internet, computer 3304 typically will have a standard top-level domain name such as .com, .net, .org, .edu, .mil or .gov.

Petitioner Apple Inc. - Exhibit 1002, p. 83

[00260] FIG. 34 shows a flow diagram 3400 for installing and establishing a "one-click" secure communication link over a computer network according to the present invention. At step 3401, computer 3301 is connected to server computer 3304 over a non-VPN communication link 3305. Web browser 3306 displays a web page associated with server 3304 in a well-known manner. According to one variation of the invention, the display of computer 3301 contains a hyperlink, or an icon representing a hyperlink, for selecting a virtual private network (VPN) communication link ("go secure" hyperlink) through computer network 3302 between terminal 3301 and server 3304. Preferably, the "go secure" hyperlink is displayed as part of the web page downloaded from server computer 3304, thereby indicating that the entity providing server 3304 also provides VPN capability.

[00261] By displaying the "go secure" hyperlink, a user at computer 3301 is informed that the current communication link between computer 3301 and server computer 3304 is a non-secure, non-VPN communication link. At step 3402, it is determined whether a user of computer 3301 has selected the "go secure" hyperlink. If not, processing resumes using a non-secure (conventional) communication method (not shown). If, at step 3402, it is determined that the user has selected the "go secure" hyperlink, flow continues to step 3403 where an object associated with the hyperlink determines whether a VPN communication software module has already been installed on computer 3301. Alternatively, a user can enter a command into computer 3301 to "go secure."

[00262] If, at step 3403, the object determines that the software module has been installed, flow continues to step 3407. If, at step 3403, the object determines that the software module has not been installed, flow continues to step 3404 where a non-VPN communication link 3307 is launched between computer 3301 and a website 3308 over computer network 3302 in a well- known manner. Website 3308 is accessible by all computer terminals connected to computer network 3302 through a non-VPN communication link. Once connected to website 3308, a software module for establishing a secure communication link over computer network 3302 can be downloaded and installed. Flow continues to step 3405 where, after computer 3301 connects to website 3308, the software module for establishing a communication link is downloaded and installed in a well-known manner on computer terminal 3301 as software

Petitioner Apple Inc. - Exhibit 1002, p. 84

module 3309. At step 3405, a user can optionally select parameters for the software module, such as enabling a secure communication link mode of communication for all communication links over computer network 3302. At step 3406, the communication link between computer 3301 and website 3308 is then terminated in a well-known manner.

[00263] By clicking on the "go secure" hyperlink, a user at computer 3301 has enabled a secure communication mode of communication between computer 3301 and server computer 3304. According to one variation of the invention, the user is not required to do anything more than merely click the "go secure" hyperlink. The user does not need to enter any user identification information, passwords or encryption keys for establishing a secure communication link. All procedures required for establishing a secure communication link between computer 3301 and server computer 3304 are performed transparently to a user at computer 3301.

[00264] At step 3407, a secure VPN communications mode of operation has been enabled and software module 3309 begins to establish a VPN communication link. In one embodiment, software module 3309 automatically replaces the top-level domain name for server 3304 within browser 3406 with a secure top-level domain name for server computer 3304. For example, if the top-level domain name for server 3304 is .com, software module 3309 replaces the .com top- level domain name with a .scom top-level domain name, where the "s" stands for secure. Alternatively, software module 3409 can replace the top-level domain name of server 3304 with any other non-standard top-level domain name.

[00265] Because the secure top-level domain name is a non-standard domain name, a query to a standard domain name service (DNS) will return a message indicating that the universal resource locator (URL) is unknown. According to the invention, software module 3409 contains the URL for querying a secure domain name service (SDNS) for obtaining the URL for a secure top-level domain name. In this regard, software module 3309 accesses a secure portal 3310 that interfaces a secure network 3311 to computer network 3302. Secure network 3311 includes an internal router 3312, a secure domain name service (SDNS) 3313, a VPN gatekeeper 3314 and a secure proxy 3315. The secure network can include other network services, such as e-mail 3316, a plurality of chatrooms (of which only one chatroom 3317 is shown), and a standard

Petitioner Apple Inc. - Exhibit 1002, p. 85

domain name service (STD DNS) 3318. Of course, secure network 3311 can include other resources and services that are not shown in FIG. 33.

[00266] When software module 3309 replaces the standard top-level domain name for server 3304 with the secure top-level domain name, software module 3309 sends a query to SDNS 3313 at step 3408 through secure portal 3310 preferably using an administrative VPN communication link 3319. In this configuration, secure portal 3310 can only be accessed using a VPN communication link. Preferably, such a VPN communication link can be based on a technique of inserting a source and destination IP address pair into each data packet that is selected according to a pseudo-random sequence; an IP address hopping regime that pseudorandomly changes IP addresses in packets transmitted between a client computer and a secure target computer; periodically changing at least one field in a series of data packets according to a known sequence; an Internet Protocol (IP) address in a header of each data packet that is compared to a table of valid IP addresses maintained in a table in the second computer; and/or a comparison of the IP address in the header of each data packet to a moving window of valid IP addresses, and rejecting data packets having IP addresses that do not fall within the moving window. Other types of VPNs can alternatively be used. Secure portal 3310 authenticates the query from software module 3309 based on the particular information hopping technique used for VPN communication link 3319.

[00267] SDNS 3313 contains a cross-reference database of secure domain names and corresponding secure network addresses. That is, for each secure domain name, SDNS 3313 stores a computer network address corresponding to the secure domain name. An entity can register a secure domain name in SDNS 3313 so that a user who desires a secure communication link to the website of the entity can automatically obtain the secure computer network address for the secure website. Moreover, an entity can register several secure domain names, with each respective secure domain name representing a different priority level of access in a hierarchy of access levels to a secure website. For example, a securities trading website can provide users secure access so that a denial of service attack on the website will be ineffectual with respect to users subscribing to the secure website service. Different levels of subscription can be arranged based on, for example, an escalating fee, so that a user can select a desired level of guarantee for

Petitioner Apple Inc. - Exhibit 1002, p. 86

connecting to the secure securities trading website. When a user queries SDNS 3313 for the secure computer network address for the securities trading website, SDNS 3313 determines the particular secure computer network address based on the user's identity and the user's subscription level.

[00268] At step 3409, SDNS 3313 accesses VPN gatekeeper 3314 for establishing a VPN communication link between software module 3309 and secure server 3320. Server 3320 can only be accessed through a VPN communication link. VPN gatekeeper 3314 provisions computer 3301 and secure web server computer 3320, or a secure edge router for server computer 3320, thereby creating the VPN. Secure server computer 3320 can be a separate server computer from server computer 3304, or can be the same server computer having both non-VPN and VPN communication link capability, such as shown by server computer 3322. Returning to FIG. 34, in step 3410, SDNS 3313 returns a secure URL to software module 3309 for the .scom server address for a secure server 3320 corresponding to server 3304.

[00269] Alternatively, SDNS 3313 can be accessed through secure portal 3310 "in the clear", that is, without using an administrative VPN communication link. In this situation, secure portal 3310 preferably authenticates the query using any well-known technique, such as a cryptographic technique, before allowing the query to proceed to SDNS 3319. Because the initial communication link in this situation is not a VPN communication link, the reply to the query can be "in the clear." The querying computer can use the clear reply for establishing a VPN link to the desired domain name. Alternatively, the query to SDNS 3313 can be in the clear, and SDNS 3313 and gatekeeper 3314 can operate to establish a VPN communication link to the querying computer for sending the reply.

[00270] At step 3411, software module 3309 accesses secure server 3320 through VPN communication link 3321 based on the VPN resources allocated by VPN gatekeeper 3314. At step 3412, web browser 3306 displays a secure icon indicating that the current communication link to server 3320 is a secure VPN communication link. Further communication between computers 3301 and 3320 occurs via the VPN, e.g., using a "hopping" regime as discussed above. When VPN link 3321 is terminated at step 3413, flow continues to step 3414 where software module 3309 automatically replaces the secure top-level domain name with the

Petitioner Apple Inc. - Exhibit 1002, p. 87

corresponding non-secure top-level domain name for server 3304. Browser 3306 accesses a standard DNS 3325 for obtaining the non-secure URL for server 3304. Browser 3306 then connects to server 3304 in a well-known manner. At step 3415, browser 3306 displays the "go secure" hyperlink or icon for selecting a VPN communication link between terminal 3301 and server 3304. By again displaying the "go secure" hyperlink, a user is informed that the current communication link is a non-secure, non-VPN communication link.

[00271] When software module 3309 is being installed or when the user is off-line, the user can optionally specify that all communication links established over computer network 3302 are secure communication links. Thus, anytime that a communication link is established, the link is a VPN link. Consequently, software module 3309 transparently accesses SDNS 3313 for obtaining the URL for a selected secure website. In other words, in one embodiment, the user need not "click" on the secure option each time secure communication is to be effected.

[00272] Additionally, a user at computer 3301 can optionally select a secure communication link through proxy computer 3315. Accordingly, computer 3301 can establish a VPN communication link 3323 with secure server computer 3320 through proxy computer 3315. Alternatively, computer 3301 can establish a non-VPN communication link 3324 to a non-secure website, such as non-secure server computer 3304.

[00273] FIG. 35 shows a flow diagram 3500 for registering a secure domain name according to the present invention. At step 3501, a requester accesses website 3308 and logs into a secure domain name registry service that is available through website 3308. At step 3502, the requestor completes an online registration form for registering a secure domain name having a top-level domain name, such as .com, .net, .org, .edu, .mil or .gov. Of course, other secure top-level domain names can also be used. Preferably, the requestor must have previously registered a non- secure domain name corresponding to the equivalent secure domain name that is being requested. For example, a requester attempting to register secure domain name "website.scom" must have previously registered the corresponding non-secure domain name "website.com".

[00274] At step 3503, the secure domain name registry service at website 3308 queries a non- secure domain name server database, such as standard DNS 3322, using, for example, a

Petitioner Apple Inc. - Exhibit 1002, p. 88

whois query, for determining ownership information relating to the non-secure domain name corresponding to the requested secure domain name. At step 3504, the secure domain name registry service at website 3308 receives a reply from standard DNS 3322 and at step 3505 determines whether there is conflicting ownership information for the corresponding non-secure domain name. If there is no conflicting ownership information, flow continues to step 3507, otherwise flow continues to step 3506 where the requestor is informed of the conflicting ownership information. Flow returns to step 3502.

[00275] When there is no conflicting ownership information at step 3505, the secure domain name registry service (website 3308) informs the requestor that there is no conflicting ownership information and prompts the requestor to verify the information entered into the online form and select an approved form of payment. After confirmation of the entered information and appropriate payment information, flow continues to step 3508 where the newly registered secure domain name sent to SDNS 3313 over communication link 3326.

[00276] If, at step 3505, the requested secure domain name does not have a corresponding equivalent non-secure domain name, the present invention informs the requestor of the situation and prompts the requestor for acquiring the corresponding equivalent non-secure domain name for an increased fee. By accepting the offer, the present invention automatically registers the corresponding equivalent non-secure domain name with standard DNS 3325 in a well-known manner. Flow then continues to step 3508.

G. Tunneling Secure Address Hopping Protocol Through Existing Protocol Using Web Proxy

[00277] The present invention also provides a technique for implementing the field hopping schemes described above in an application program on the client side of a firewall between two computer networks, and in the network stack on the server side of the firewall. The present invention uses a new secure connectionless protocol that provides good denial of service rejection capabilities by layering the new protocol on top of an existing IP protocol, such as the ICMP, UDP or TCP protocols. Thus, this aspect of the present invention does not require changes in the Internet infrastructure.

Petitioner Apple Inc. - Exhibit 1002, p. 89

[00278] According to the invention, communications are protected by a client-side proxy application program that accepts unencrypted, unprotected communication packets from a local browser application. The client-side proxy application program tunnels the unencrypted, unprotected communication packets through a new protocol, thereby protecting the communications from a denial of service at the server side. Of course, the unencrypted, unprotected communication packets can be encrypted prior to tunneling.

[00279] The client-side proxy application program is not an operating system extension and does not involve any modifications to the operating system network stack and drivers. Consequently, the client is easier to install, remove and support in comparison to a VPN. Moreover, the client- side proxy application can be allowed through a corporate firewall using a much smaller "hole" in the firewall and is less of a security risk in comparison to allowing a protocol layer VPN through a corporate firewall.

[00280] The server-side implementation of the present invention authenticates valid field-hopped packets as valid or invalid very early in the server packet processing, similar to a standard virtual private network, for greatly minimizing the impact of a denial of service attempt in comparison to normal TCP/IP and HTTP communications, thereby protecting the server from invalid communications.

[00281] FIG. 36 shows a system block diagram of a computer network 3600 in which a virtual private connection according to the present invention can be configured to more easily traverse a firewall between two computer networks. FIG. 37 shows a flow diagram 3700 for establishing a virtual private connection that is encapsulated using an existing network protocol.

[00282] In FIG. 36 a local area network (LAN) 3601 is connected to another computer network 3602, such as the Internet, through a firewall arrangement 3603. Firewall arrangement operates in a well-known manner to interface LAN 3601 to computer network 3602 and to protect LAN 3601 from attacks initiated outside of LAN 3601.

[00283] A client computer 3604 is connected to LAN 3601 in a well-known manner. Client computer 3604 includes an operating system 3605 and a web browser 3606. Operating

Petitioner Apple Inc. - Exhibit 1002, p. 90

system 3605 provides kernel mode functions for operating client computer 3604. Browser 3606 is an application program for accessing computer network resources connected to LAN 3601 and computer network 3602 in a well-known manner. According to the present invention, a proxy application 3607 is also stored on client computer 3604 and operates at an application layer in conjunction with browser 3606. Proxy application 3607 operates at the application layer within client computer 3604 and when enabled, modifies unprotected, unencrypted message packets generated by browser 3606 by inserting data into the message packets that are used for forming a virtual private connection between client computer 3604 and a server computer connected to LAN 3601 or computer network 3602. According to the invention, a virtual private connection does not provide the same level of security to the client computer as a virtual private network. A virtual private connection can be conveniently authenticated so that, for example, a denial of service attack can be rapidly rejected, thereby providing different levels of service that can be subscribed to by a user.

[00284] Proxy application 3607 is conveniently installed and uninstalled by a user because proxy application 3607 operates at the application layer within client computer 3604. On installation, proxy application 3607 preferably configures browser 3606 to use proxy application for all web communications. That is, the payload portion of all message packets is modified with the data for forming a virtual private connection between client computer 3604 and a server computer. Preferably, the data for forming the virtual private connection contains field-hopping data, such as described above in connection with VPNs. Also, the modified message packets preferably conform to the UDP protocol. Alternatively, the modified message packets can conform to the TCP/IP protocol or the ICMP protocol. Alternatively, proxy application 3606 can be selected and enabled through, for example, an option provided by browser 3606. Additionally, proxy application 3607 can be enabled so that only the payload portion of specially designated message packets is modified with the data for forming a virtual private connection between client computer 3604 and a designated host computer. Specially designated message packets can be, for example, selected predetermined domain names.

[00285] Referring to FIG. 37, at step 3701, unprotected and unencrypted message packets are generated by browser 3606. At step 3702, proxy application 3607 modifies the

Petitioner Apple Inc. - Exhibit 1002, p. 91

payload portion of all message packets by tunneling the data for forming a virtual private connection between client computer 3604 and a destination server computer into the payload portion. At step, 3703, the modified message packets are sent from client computer 3604 to, for example, website (server computer) 3608 over computer network 3602.

[00286] Website 3608 includes a VPN guard portion 3609, a server proxy portion 3610 and a web server portion 3611. VPN guard portion 3609 is embedded within the kernel layer of the operating system of website 3608 so that large bandwidth attacks on website 3608 are rapidly rejected. When client computer 3604 initiates an authenticated connection to website 3608, VPN guard portion 3609 is keyed with the hopping sequence contained in the message packets from client computer 3604, thereby performing a strong authentication of the client packet streams entering website 3608 at step 3704. VPN guard portion 3609 can be configured for providing different levels of authentication and, hence, quality of service, depending upon a subscribed level of service. That is, VPN guard portion 3609 can be configured to let all message packets through until a denial of service attack is detected, in which case VPN guard portion 3609 would allow only client packet streams conforming to a keyed hopping sequence, such as that of the present invention.

[00287] Server proxy portion 3610 also operates at the kernel layer within website 3608 and catches incoming message packets from client computer 3604 at the VPN level. At step 3705, server proxy portion 3610 authenticates the message packets at the kernel level within host computer 3604 using the destination IP address, UDP ports and discriminator fields. The authenticated message packets are then forwarded to the authenticated message packets to web server portion 3611 as normal TCP web transactions.

[00288] At step 3705, web server portion 3611 responds to message packets received from client computer 3604 in accordance with the particular nature of the message packets by generating reply message packets. For example, when a client computer requests a webpage, web server portion 3611 generates message packets corresponding to the requested webpage. At step 3706, the reply message packets pass through server proxy portion 3610, which inserts data into the payload portion of the message packets that are used for forming the virtual private connection between host computer 3608 and client computer 3604 over computer network 3602.

Petitioner Apple Inc. - Exhibit 1002, p. 92

Preferably, the data for forming the virtual private connection is contains field-hopping data, such as described above in connection with VPNs. Server proxy portion 3610 operates at the kernel layer within host computer 3608 to insert the virtual private connection data into the payload portion of the reply message packets. Preferably, the modified message packets sent by host computer 3608 to client computer 3604 conform to the UDP protocol. Alternatively, the modified message packets can conform to the TCP/IP protocol or the ICMP protocol.

[00289] At step 3707, the modified packets are sent from host computer 3608 over computer network 3602 and pass through firewall 3603. Once through firewall 3603, the modified packets are directed to client computer 3604 over LAN 3601 and are received at step 3708 by proxy application 3607 at the application layer within client computer 3604. Proxy application 3607 operates to rapidly evaluate the modified message packets for determining whether the received packets should be accepted or dropped. If the virtual private connection data inserted into the received information packets conforms to expected virtual private connection data, then the received packets are accepted. Otherwise, the received packets are dropped.

[00290] While the present invention has been described in connection with the illustrated embodiments, it will be appreciated and understood that modifications may be made without departing from the true spirit and scope of the invention.

CLAIMS

What is claimed is:

1. A network device, comprising:

a storage device storing an application program for a secure communications service; and

at least one processor configured to execute the application program for the secure communications service so as to enable the network device to:

send a request to look up a network address of a second network device based on an identifier associated with the second network device;

receive an indication that the second network device is available for the secure communications service, the indication including the requested network address of the second network device and provisioning information for a virtual private network communication link;

connect to the second network device, using the received network address of the second network device and the provisioning information for the virtual private network communication link; and

communicate with the second network device using the secure communications service via the virtual private network communication link.

2. The network device of claim 1, wherein:

the secure communications service includes an audio-video conferencing service; and

the at least one processor is configured to execute the secure communications service application program so as to allow the network device to communicate data using the audio-video conferencing service.

3. The network device of claim 1, wherein the at least one processor is configured to execute the application program so that at least one of video data and audio data can be communicated over the virtual private network communication link using the audio-video conferencing service.

Petitioner Apple Inc. - Exhibit 1002, p. 94

4. The network device of claim 1, wherein the secure communications service includes a messaging service.

5. The network device of claim 4, wherein the messaging service includes an e-mail service.

6. The network device of claim 1, wherein the secure communications service includes a telephony service.

7. The system of claim 6, wherein the telephony service uses modulation.

8. The network device of claim 7, wherein the modulation is based on one of frequency-division multiplexing (FDM), time-division multiplexing (TDM), or code division multiple access (CDMA).

9. The network device of claim 1, wherein the network device is a mobile device.

10. The network device of claim 9, wherein the mobile device is a notebook computer.

11. The network device of claim 1, wherein the identifier associated with the second network device is a domain name.

12. The network device of claim 1, wherein the virtual private network communication link is based on inserting into each data packet communicated over the virtual private network communication link one or more data values that vary according to a pseudo-random sequence.

13. The network device of claim 1, wherein the virtual private network communication link is based on a network address hopping regime that is used to pseudo-randomly change network addresses in packets transmitted between a first device and a second device.

14. The network device of claim 1, wherein the indication that the second network device is available for the secure communications service is a function of the result of a domain name lookup.

15. A method executed by a first network device for communicating with a second network device, the method comprising:

sending a request to look up a network address of a second network device based on an identifier associated with the second network device;

receiving an indication that the second network device is available for a secure communications service, the indication including the requested network address of the second network device and provisioning information for a virtual private network communication link; and

connecting to the second network device over the virtual private network communication link, using the received network address of the second network device and the provisioning information for the virtual private network communication link; and

communicating with the second network device using the secure communications service via the virtual private network communication link.

16. The method of claim 15, wherein the secure communications service includes a video conferencing service, and communicating includes communicating at least one of video data and audio data using the video conferencing service.

17. The method of claim 15, further comprising encrypting at least one of the video data and audio data over the virtual private network communication link.

18. The method of claim 15, wherein the secure communications service includes a messaging service.

19. The method of claim 18, wherein the messaging service includes an e-mail service.

20. The method of claim 15, wherein the secure communications service includes a telephony service.

Petitioner Apple Inc. - Exhibit 1002, p. 96

21. The method of claim 20, wherein the telephony service uses modulation.

22. The method of claim 21, wherein the modulation is based on one of frequency-division multiplexing (FDM), time-division multiplexing (TDM), or code division multiple access (CDMA).

23. The method of claim 15, wherein the network device is a mobile device.

24. The method of claim 23, wherein the mobile device is a notebook computer.

25. The method of claim 15, wherein the identifier associated with the second network device is a domain name.

26. The method of claim 15, wherein communicating with the second network device using the secure communications service via the virtual private network communication link includes inserting into data packets communicated over the virtual private network communication link one or more data values that vary according to a pseudo-random sequence.

27. The method of claim 15, wherein communicating with the second network device using the secure communications service via the virtual private network communication link includes network address hopping regime that is used to pseudorandomly change network addresses in packets transmitted between a first device and a second device.

28. The method of claim 15, wherein the indication that the second network device is available for a secure communications service is a function of a domain name lookup.

Petitioner Apple Inc. - Exhibit 1002, p. 97

ABSTRACT

A network device comprises: a storage device storing an application program for a secure communications service; and at least one processor configured to execute the application program for the secure communications service so as to enable the network device to (a) send a request to look up a network address of a second network device based on an identifier associated with the second network device; (b) receive an indication that the second network device is available for the secure communications service, the indication including the requested network address of the second network device and provisioning information for a virtual private network communication link; (c) connect to the second network device, using the received network address of the second network device and the provisioning information for the virtual private network communication link; and (d) communicate with the second network device using the secure communications service via the virtual private network communication link.

Petitioner Apple Inc. - Exhibit 1002, p. 98

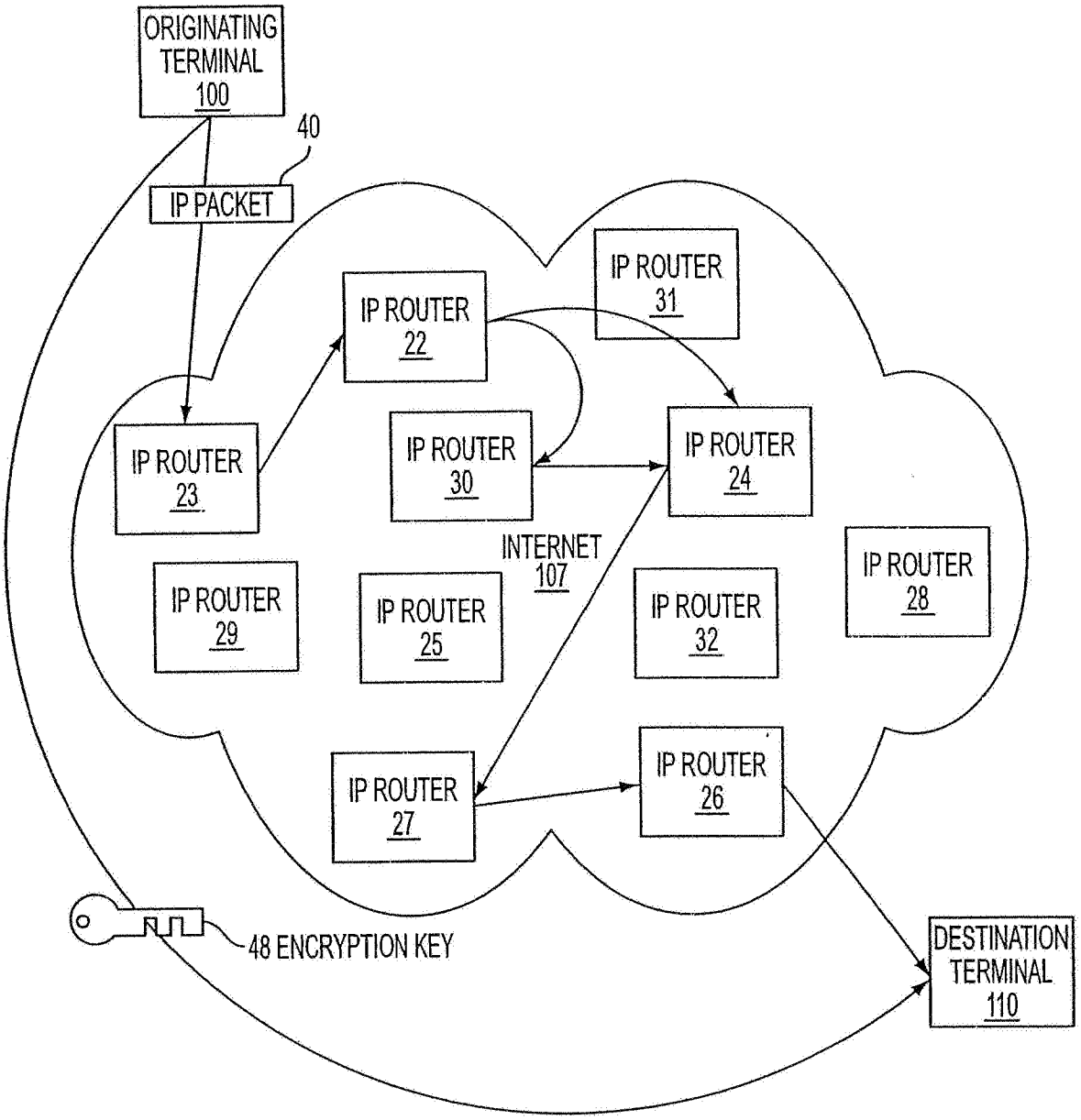

ORIGINATING TERMINAL 100
40
IP PACKET
IP ROUTER 22
IP ROUTER 31
IP ROUTER 23
IP ROUTER 30
IP ROUTER 24
INTERNET 107
IP ROUTER 29
IP ROUTER 25
IP ROUTER 32
IP ROUTER 28
IP ROUTER 27
IP ROUTER 26
48 ENCRYPTION KEY
DESTINATION TERMINAL 110

FIG. 1

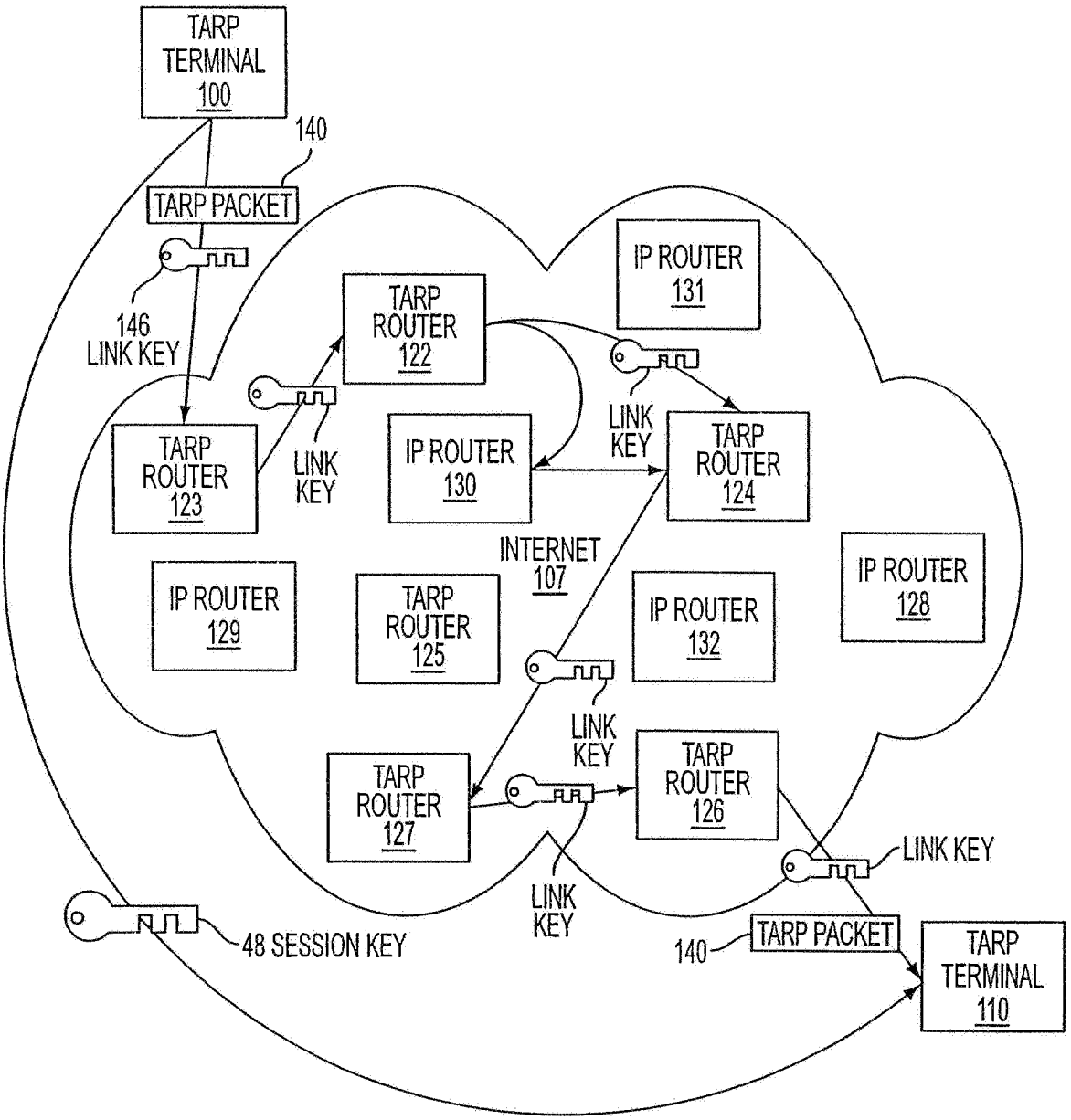

TARP TERMINAL 100
140
TARP PACKET
146 LINK KEY
TARP ROUTER 122
IP ROUTER 131
LINK KEY
TARP ROUTER 123
LINK KEY
IP ROUTER 130
LINK KEY
TARP ROUTER 124
INTERNET 107
IP ROUTER 129
TARP ROUTER 125
IP ROUTER 132
IP ROUTER 128
LINK KEY
TARP ROUTER 127
TARP ROUTER 126
LINK KEY
LINK KEY
48 SESSION KEY
140
TARP PACKET
TARP TERMINAL 110

FIG. 2

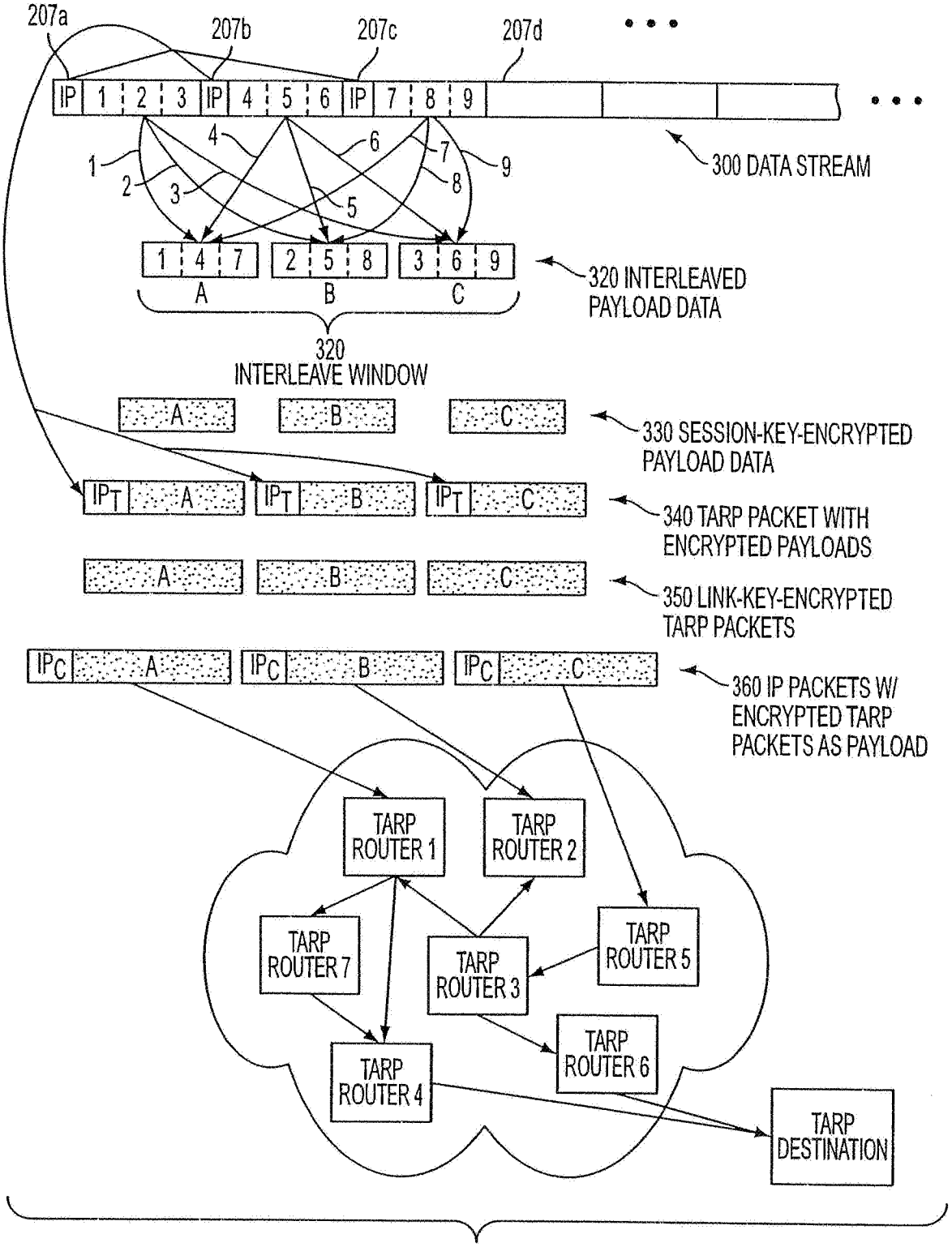

207a
207b
207c
207d
IP 1 2 3 IP 4 5 6 IP 7 8 9
300 DATA STREAM
1 2 3 4 5 6 7 8 9
1 4 7
2 5 8
3 6 9
A
B
C
320 INTERLEAVED PAYLOAD DATA
320 INTERLEAVE WINDOW
330 SESSION-KEY-ENCRYPTED PAYLOAD DATA
IPT A
IPT B
IPT C
340 TARP PACKET WITH ENCRYPTED PAYLOADS
350 LINK-KEY-ENCRYPTED TARP PACKETS
IPC A
IPC B
IPC C
360 IP PACKETS W/ ENCRYPTED TARP PACKETS AS PAYLOAD
TARP ROUTER 1
TARP ROUTER 2
TARP ROUTER 7
TARP ROUTER 3
TARP ROUTER 5
TARP ROUTER 4
TARP ROUTER 6
TARP DESTINATION

FIG. 3A

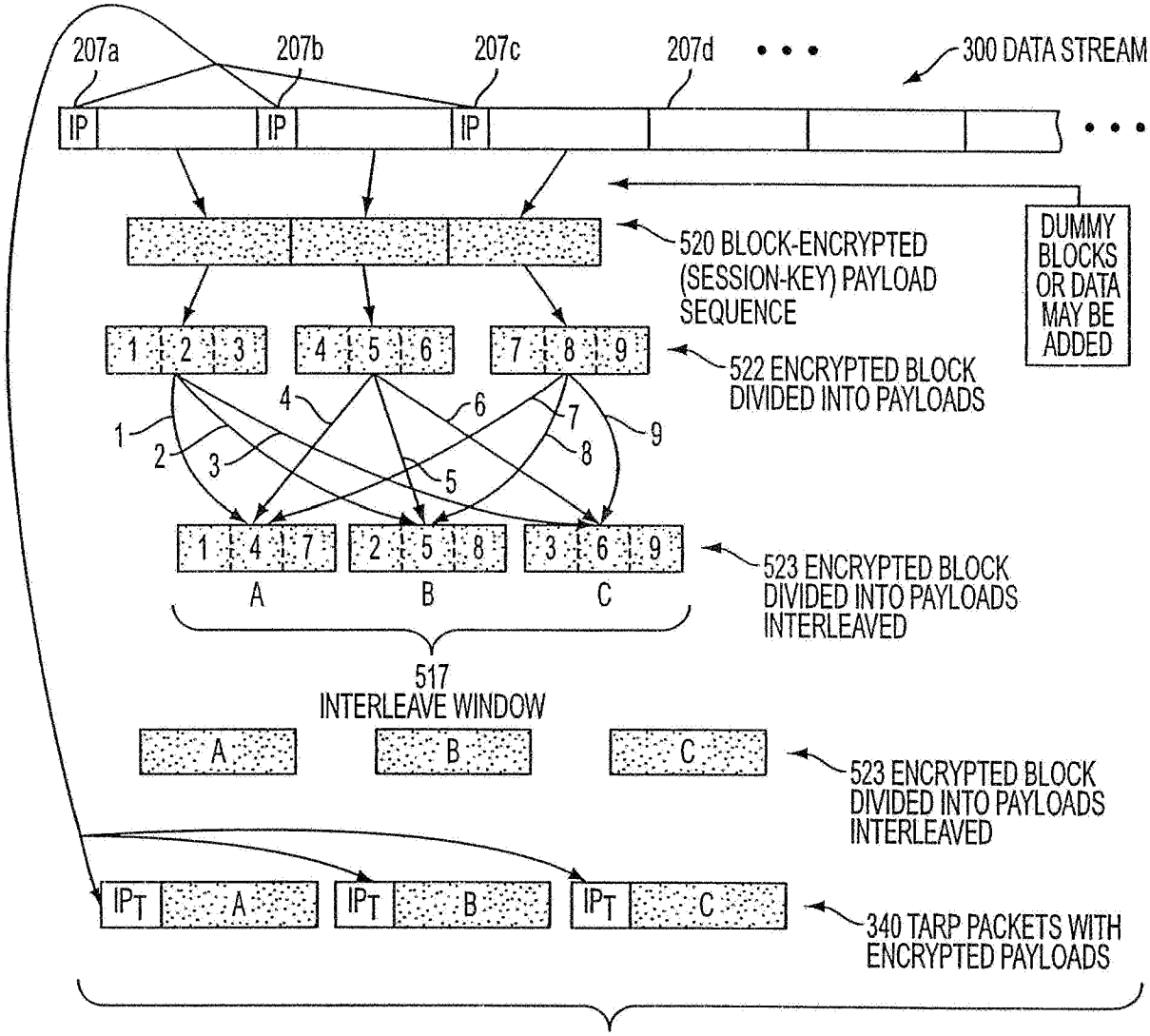

207a
207b
207c
207d
300 DATA STREAM
IP
IP
IP
520 BLOCK-ENCRYPTED (SESSION-KEY) PAYLOAD SEQUENCE
DUMMY BLOCKS OR DATA MAY BE ADDED
1 2 3
4 5 6
7 8 9
522 ENCRYPTED BLOCK DIVIDED INTO PAYLOADS
1 4 7
2 5 8
3 6 9
A
B
C
523 ENCRYPTED BLOCK DIVIDED INTO PAYLOADS INTERLEAVED
517
INTERLEAVE WINDOW
523 ENCRYPTED BLOCK DIVIDED INTO PAYLOADS INTERLEAVED
IPT
340 TARP PACKETS WITH ENCRYPTED PAYLOADS

FIG. 3B

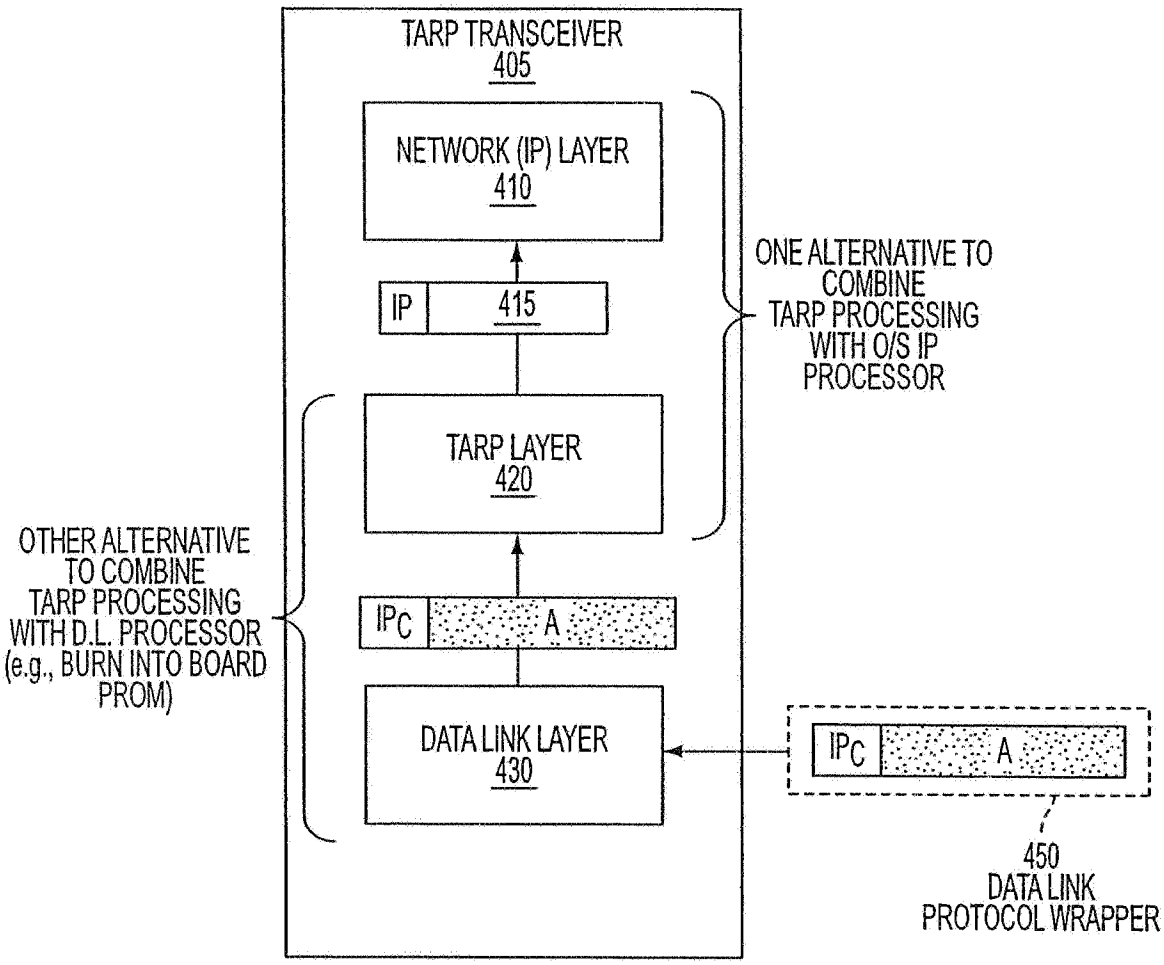

TARP TRANSCEIVER
405
NETWORK (IP) LAYER
410
IP
415
TARP LAYER
420
IPC
A
DATA LINK LAYER
430
ONE ALTERNATIVE TO COMBINE TARP PROCESSING WITH O/S IP PROCESSOR
OTHER ALTERNATIVE TO COMBINE TARP PROCESSING WITH D.L. PROCESSOR (e.g., BURN INTO BOARD PROM)
IPC
A
450
DATA LINK PROTOCOL WRAPPER

FIG. 4

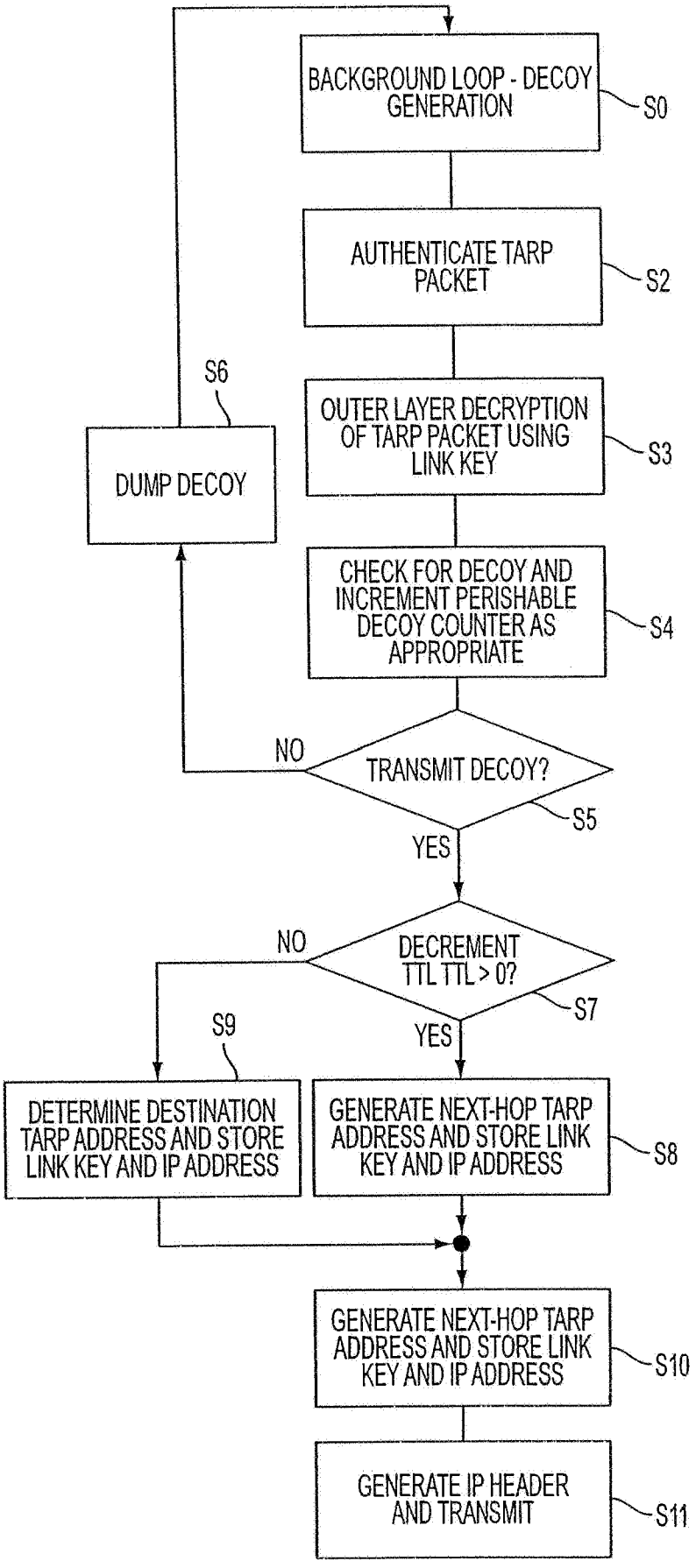

BACKGROUND LOOP - DECOY GENERATION
S0
AUTHENTICATE TARP PACKET
S2
OUTER LAYER DECRYPTION OF TARP PACKET USING LINK KEY
S3
CHECK FOR DECOY AND INCREMENT PERISHABLE DECOY COUNTER AS APPROPRIATE
S4
TRANSMIT DECOY?
S5
NO
YES
S6
DUMP DECOY
DECREMENT TTL TTL > 0?
S7
NO
YES
S9
DETERMINE DESTINATION TARP ADDRESS AND STORE LINK KEY AND IP ADDRESS
GENERATE NEXT-HOP TARP ADDRESS AND STORE LINK KEY AND IP ADDRESS
S8
GENERATE NEXT-HOP TARP ADDRESS AND STORE LINK KEY AND IP ADDRESS
S10
GENERATE IP HEADER AND TRANSMIT
S11

FIG. 5

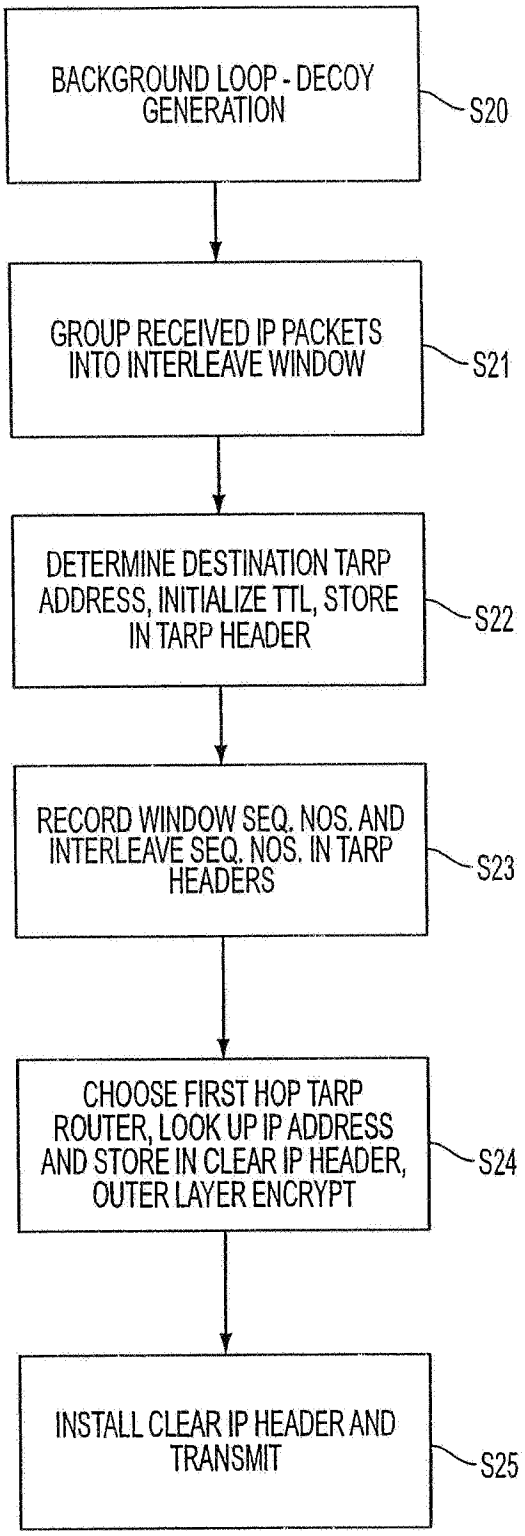

BACKGROUND LOOP - DECOY GENERATION
S20
GROUP RECEIVED IP PACKETS INTO INTERLEAVE WINDOW
S21
DETERMINE DESTINATION TARP ADDRESS, INITIALIZE TTL, STORE IN TARP HEADER
S22
RECORD WINDOW SEQ. NOS. AND INTERLEAVE SEQ. NOS. IN TARP HEADERS
S23
CHOOSE FIRST HOP TARP ROUTER, LOOK UP IP ADDRESS AND STORE IN CLEAR IP HEADER, OUTER LAYER ENCRYPT
S24
INSTALL CLEAR IP HEADER AND TRANSMIT
S25

FIG. 6

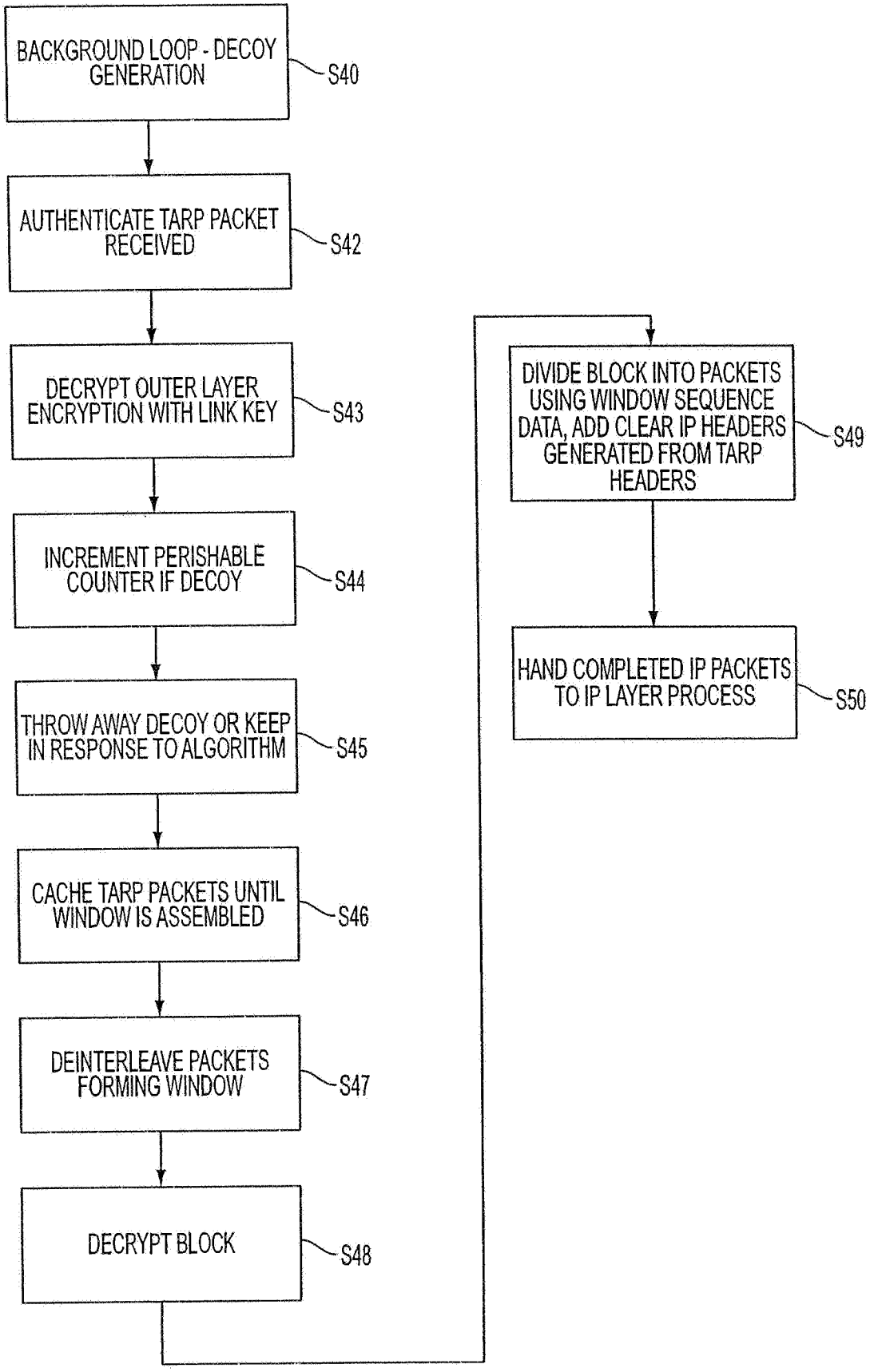

BACKGROUND LOOP - DECOY GENERATION
S40
AUTHENTICATE TARP PACKET RECEIVED
S42
DECRYPT OUTER LAYER ENCRYPTION WITH LINK KEY
S43
INCREMENT PERISHABLE COUNTER IF DECOY
S44
THROW AWAY DECOY OR KEEP IN RESPONSE TO ALGORITHM
S45
CACHE TARP PACKETS UNTIL WINDOW IS ASSEMBLED
S46
DEINTERLEAVE PACKETS FORMING WINDOW
S47
DECRYPT BLOCK
S48
DIVIDE BLOCK INTO PACKETS USING WINDOW SEQUENCE DATA, ADD CLEAR IP HEADERS GENERATED FROM TARP HEADERS
S49
HAND COMPLETED IP PACKETS TO IP LAYER PROCESS
S50

FIG. 7

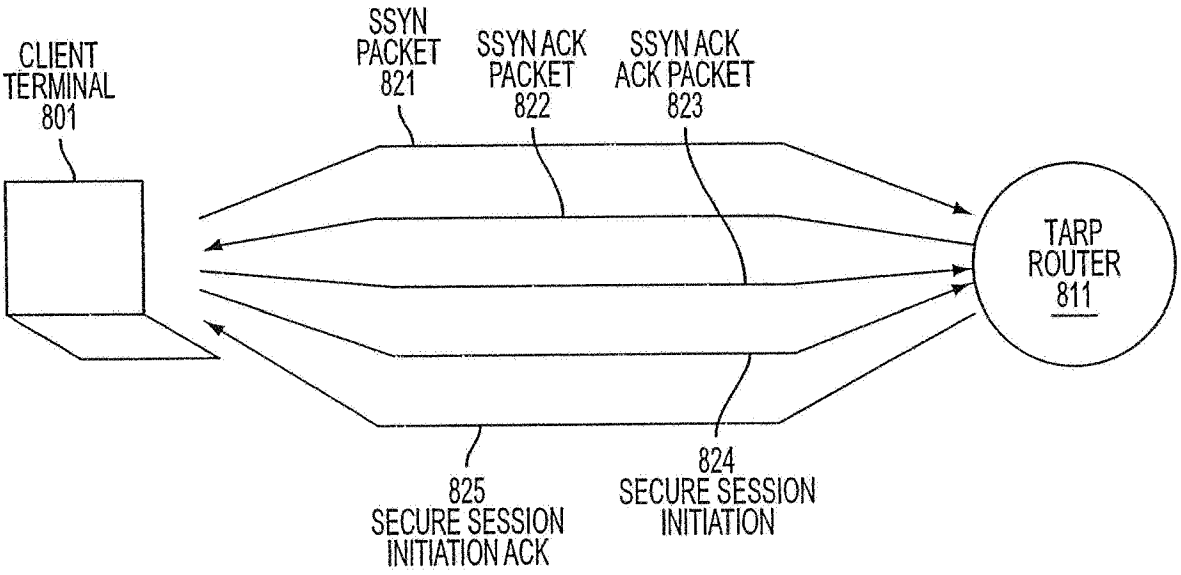

CLIENT TERMINAL 801
SSYN PACKET 821
SSYN ACK PACKET 822
SSYN ACK ACK PACKET 823
TARP ROUTER 811
825 SECURE SESSION INITIATION ACK
824 SECURE SESSION INITIATION

FIG. 8

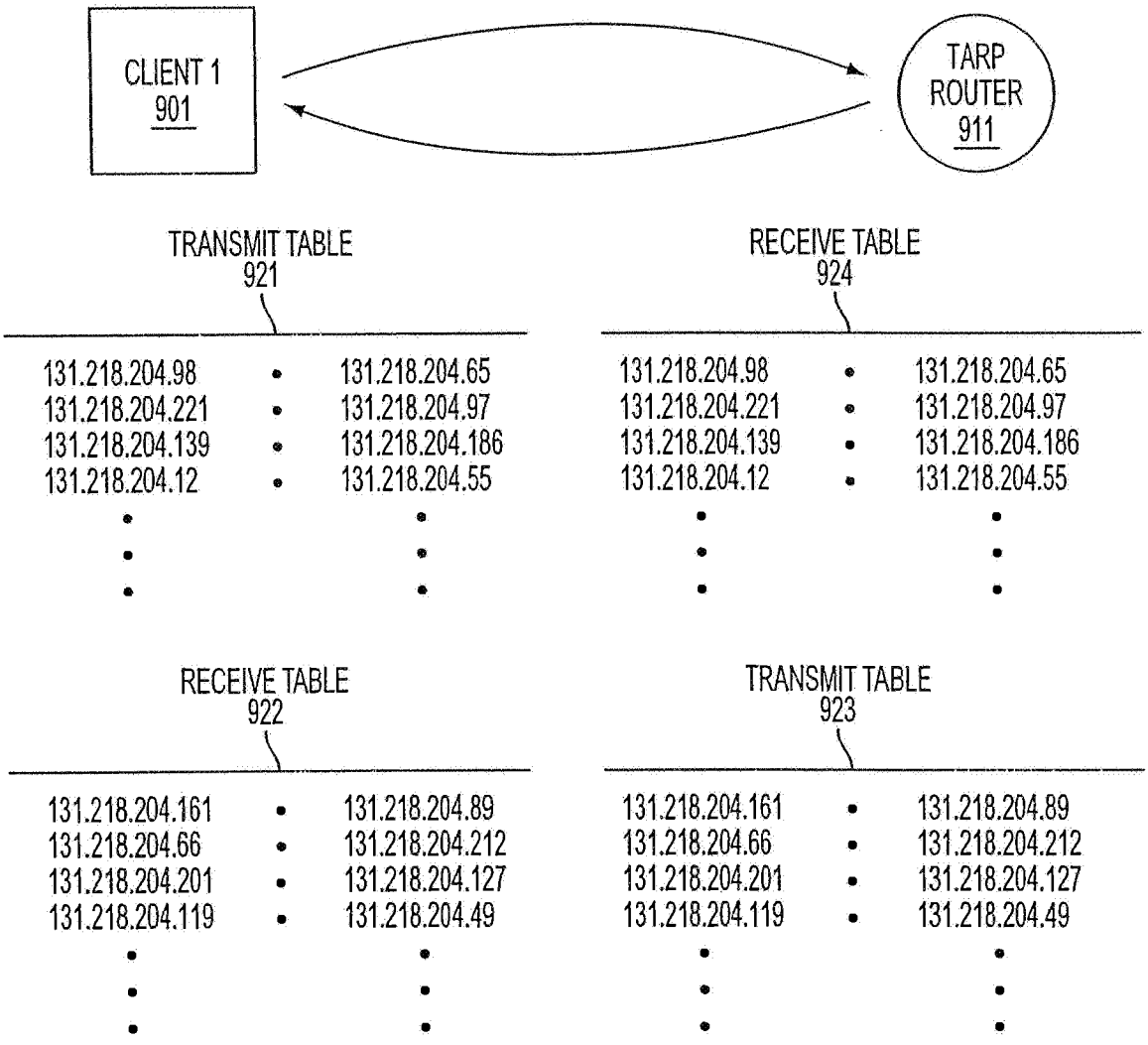

CLIENT 1
901
TARP
ROUTER
911
TRANSMIT TABLE
921
131.218.204.98 • 131.218.204.65
131.218.204.221 • 131.218.204.97
131.218.204.139 • 131.218.204.186
131.218.204.12 • 131.218.204.55
RECEIVE TABLE
924
131.218.204.98 • 131.218.204.65
131.218.204.221 • 131.218.204.97
131.218.204.139 • 131.218.204.186
131.218.204.12 • 131.218.204.55
RECEIVE TABLE
922
131.218.204.161 • 131.218.204.89
131.218.204.66 • 131.218.204.212
131.218.204.201 • 131.218.204.127
131.218.204.119 • 131.218.204.49
TRANSMIT TABLE
923
131.218.204.161 • 131.218.204.89
131.218.204.66 • 131.218.204.212
131.218.204.201 • 131.218.204.127
131.218.204.119 • 131.218.204.49

FIG. 9

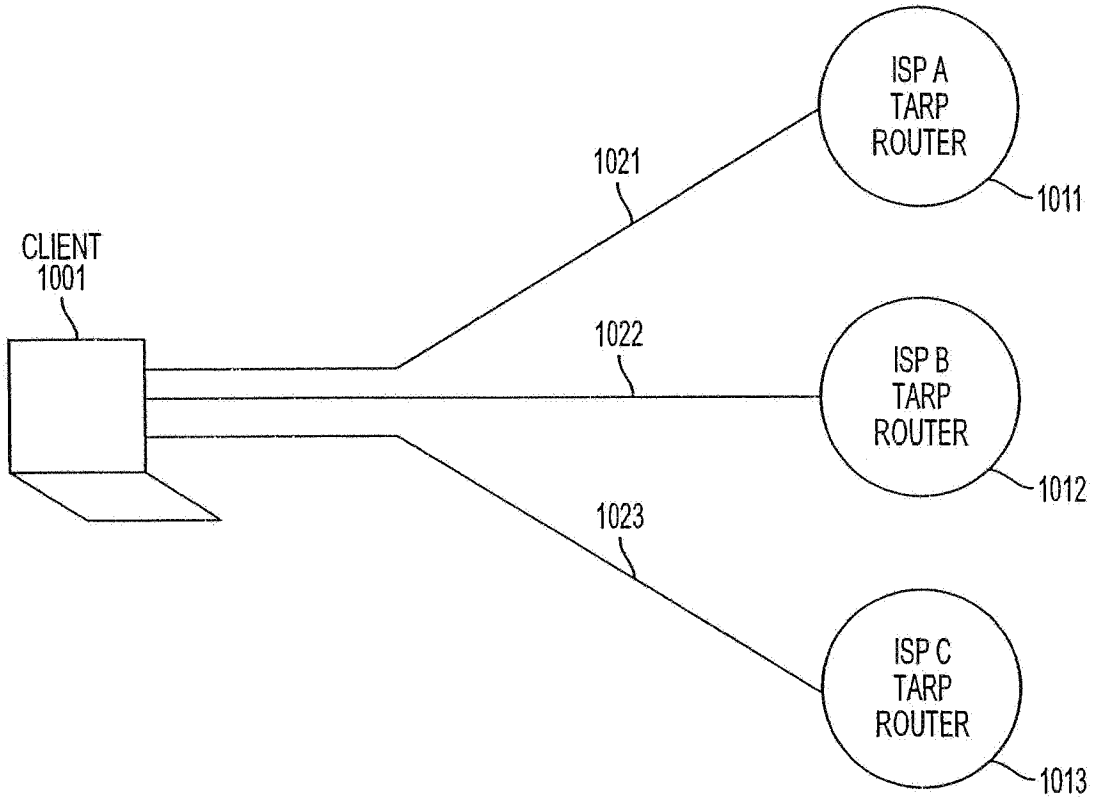

ISP A
TARP
ROUTER
1011
1021
CLIENT
1001
1022
ISP B
TARP
ROUTER
1012
1023
ISP C
TARP
ROUTER
1013

FIG. 10

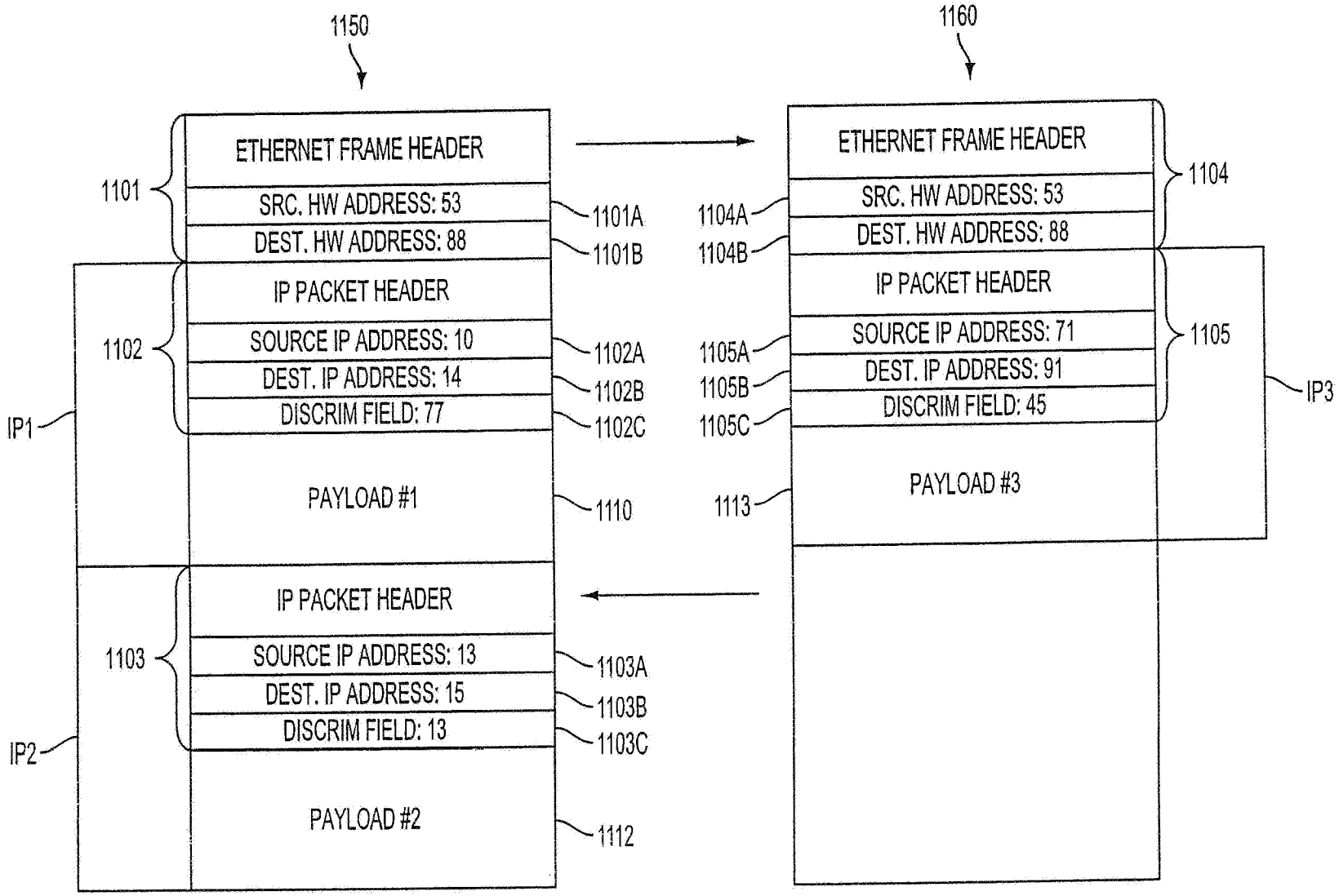


FIG. 11

Petitioner Apple Inc. - Exhibit 1002, p. 110

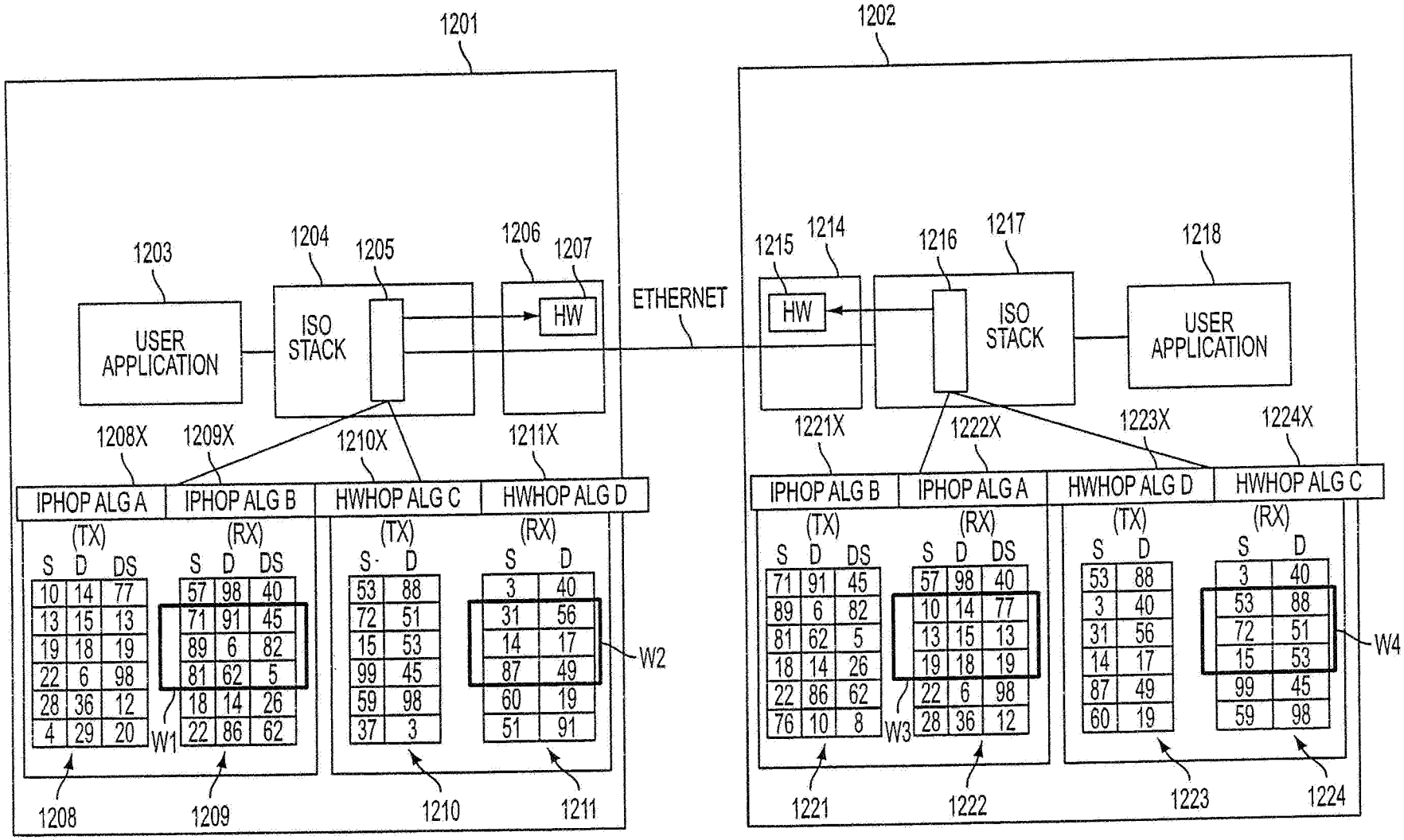


FIG. 12A

Petitioner Apple Inc. - Exhibit 1002, p. 111

MODE OR EMBODIMENT	HARDWARE ADDRESSES	IP ADDRESSES	DISCRIMINATOR FIELD VALUES
1. PROMISCUOUS	SAME FOR ALL NODES OR COMPLETELY RANDOM	CAN BE VARIED IN SYNC	CAN BE VARIED IN SYNC
2. PROMISCUOUS PER VPN	FIXED FOR EACH VPN	CAN BE VARIED IN SYNC	CAN BE VARIED IN SYNC
3. HARDWARE HOPPING	CAN BE VARIED IN SYNC	CAN BE VARIED IN SYNC	CAN BE VARIED IN SYNC

FIG. 12B

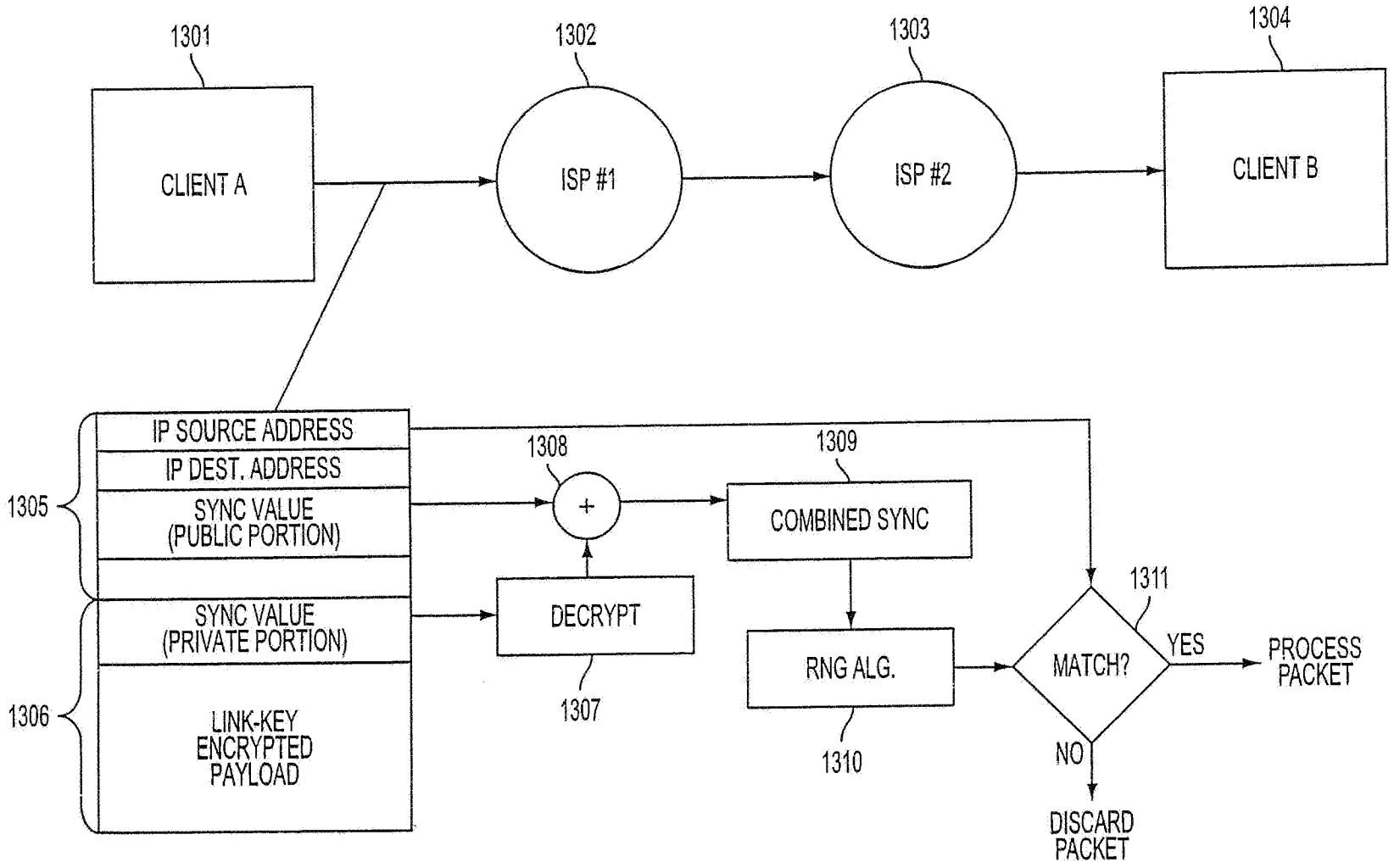


FIG. 13

Petitioner Apple Inc. - Exhibit 1002, p. 113

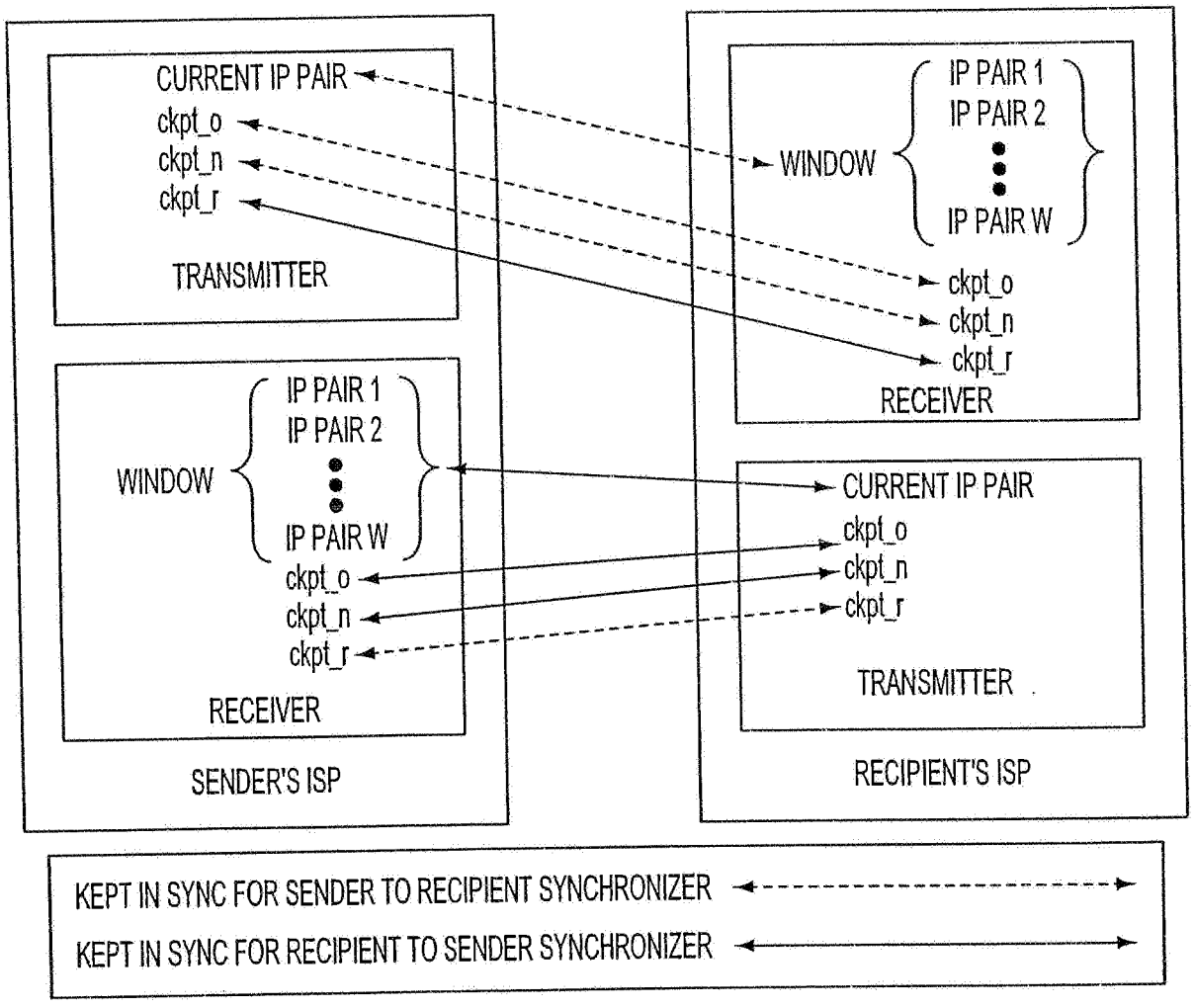

CURRENT IP PAIR
ckpt_o
ckpt_n
ckpt_r
TRANSMITTER
WINDOW
IP PAIR 1
IP PAIR 2
IP PAIR W
RECEIVER
SENDER'S ISP
WINDOW
IP PAIR 1
IP PAIR 2
IP PAIR W
ckpt_o
ckpt_n
ckpt_r
RECEIVER
CURRENT IP PAIR
ckpt_o
ckpt_n
ckpt_r
TRANSMITTER
RECIPIENT'S ISP
KEPT IN SYNC FOR SENDER TO RECIPIENT SYNCHRONIZER
KEPT IN SYNC FOR RECIPIENT TO SENDER SYNCHRONIZER

FIG. 14

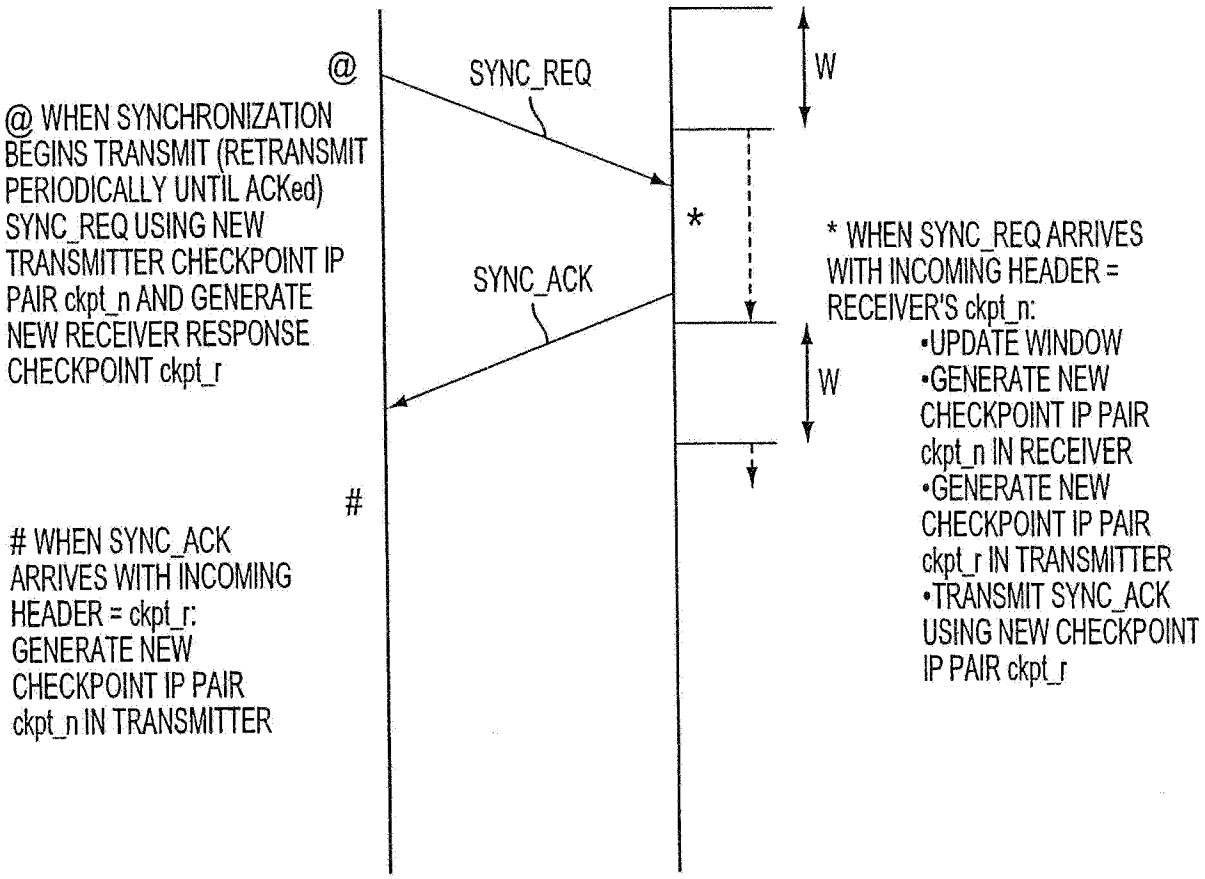

@
SYNC_REQ
W
@ WHEN SYNCHRONIZATION BEGINS TRANSMIT (RETRANSMIT PERIODICALLY UNTIL ACKed) SYNC_REQ USING NEW TRANSMITTER CHECKPOINT IP PAIR ckpt_n AND GENERATE NEW RECEIVER RESPONSE CHECKPOINT ckpt_r
*
* WHEN SYNC_REQ ARRIVES WITH INCOMING HEADER = RECEIVER'S ckpt_n:
•UPDATE WINDOW
•GENERATE NEW CHECKPOINT IP PAIR ckpt_n IN RECEIVER
•GENERATE NEW CHECKPOINT IP PAIR ckpt_r IN TRANSMITTER
•TRANSMIT SYNC_ACK USING NEW CHECKPOINT IP PAIR ckpt_r
SYNC_ACK
W
#
WHEN SYNC_ACK ARRIVES WITH INCOMING HEADER = ckpt_r: GENERATE NEW CHECKPOINT IP PAIR ckpt_n IN TRANSMITTER

FIG. 15

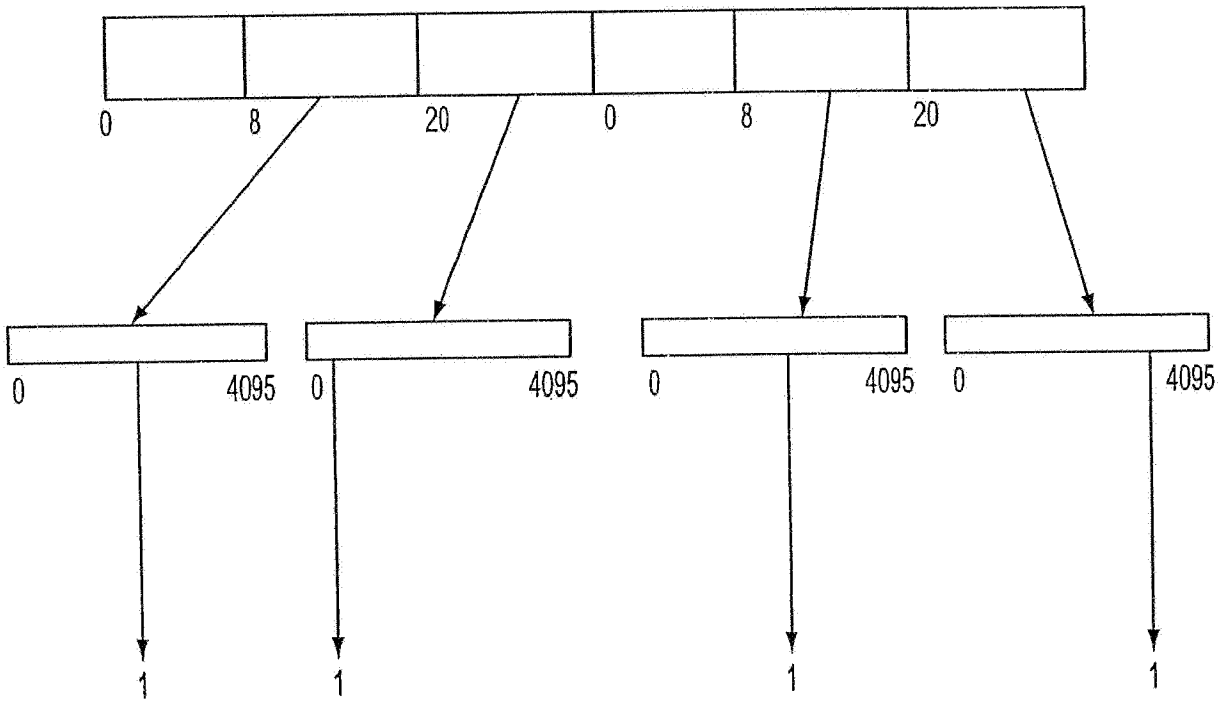


FIG. 16

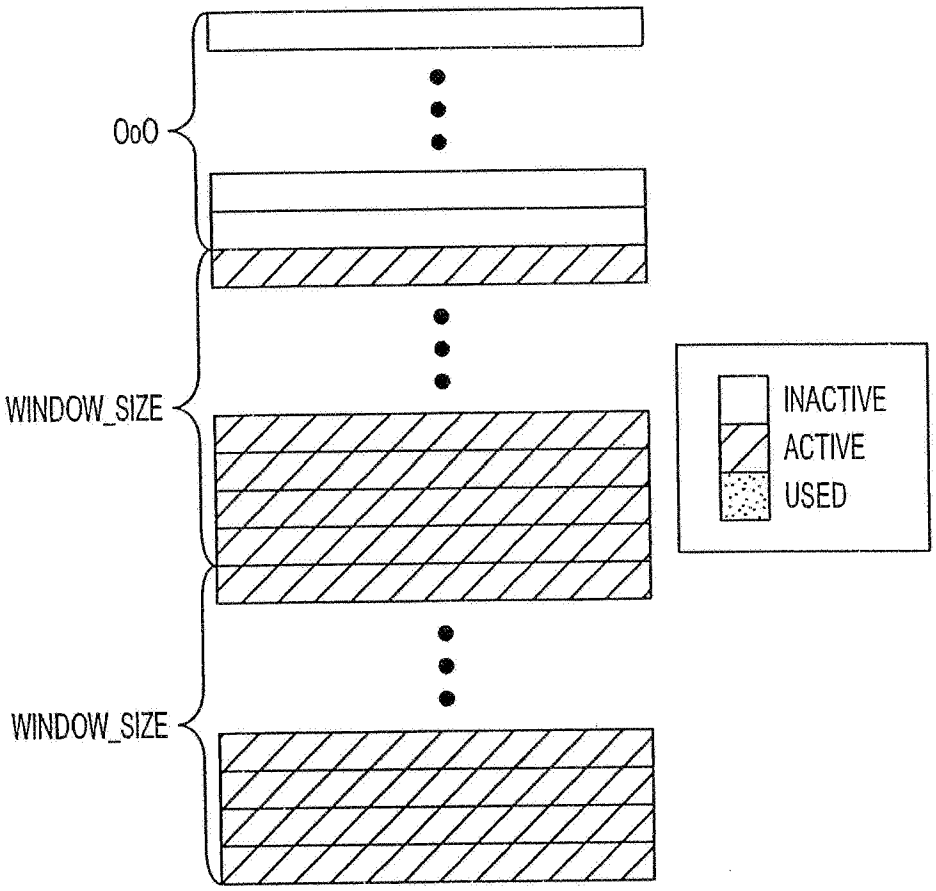


FIG. 17

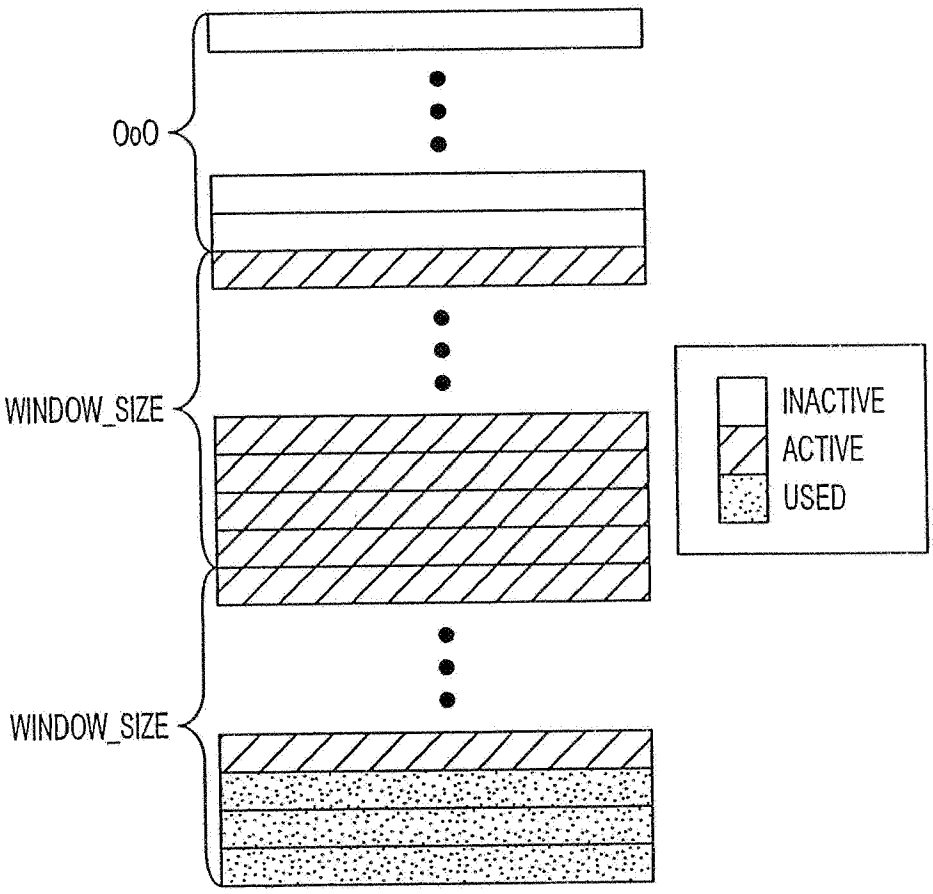


FIG. 18

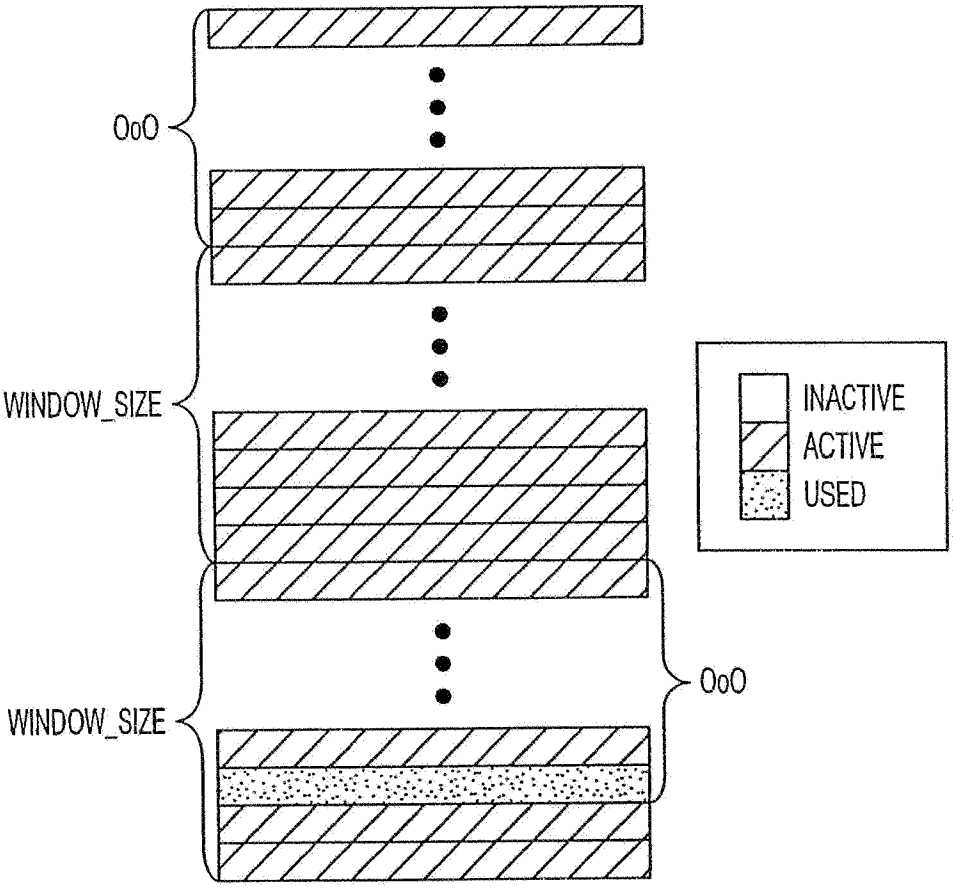


FIG. 19

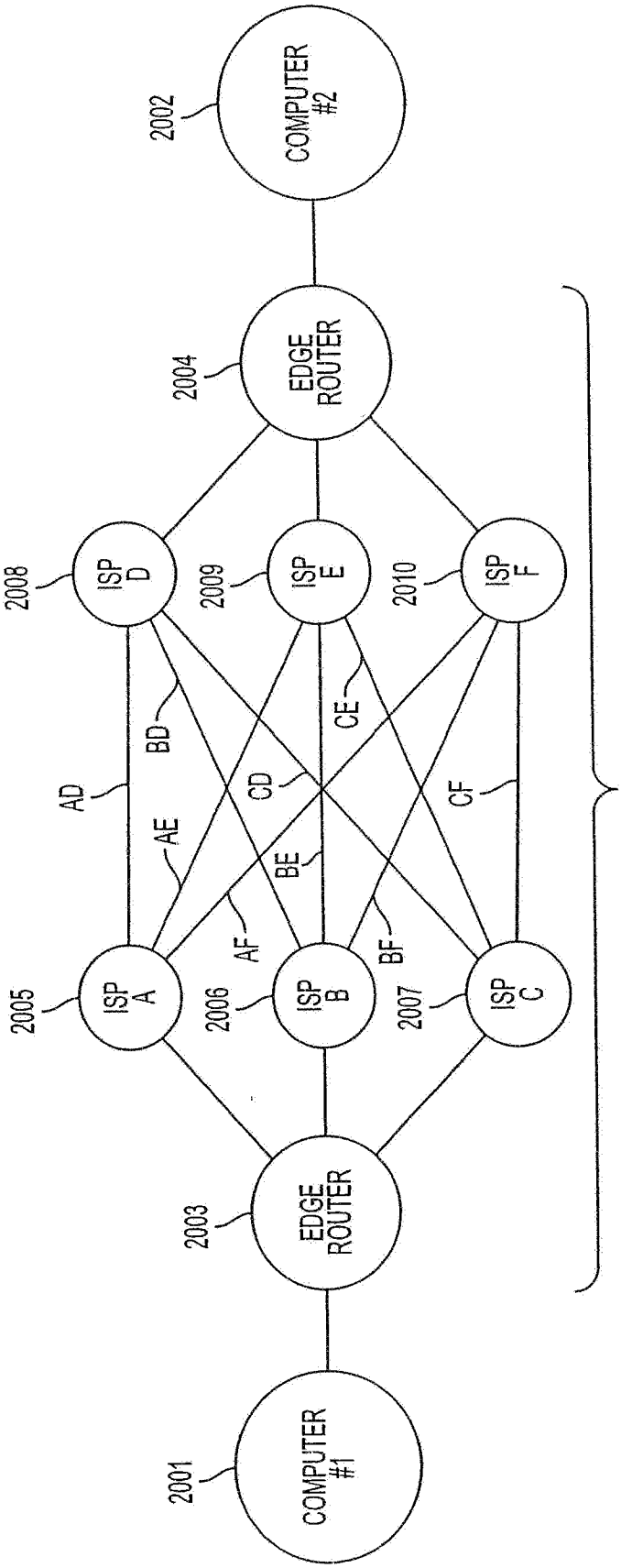

2002
COMPUTER #2
2004
EDGE ROUTER
2008
ISP D
2009
ISP E
2010
ISP F
AD
BD
CD
CE
CF
AE
AF
BE
BF
2005
ISP A
2006
ISP B
2007
ISP C
2003
EDGE ROUTER
2001
COMPUTER #1
2011

FIG. 20

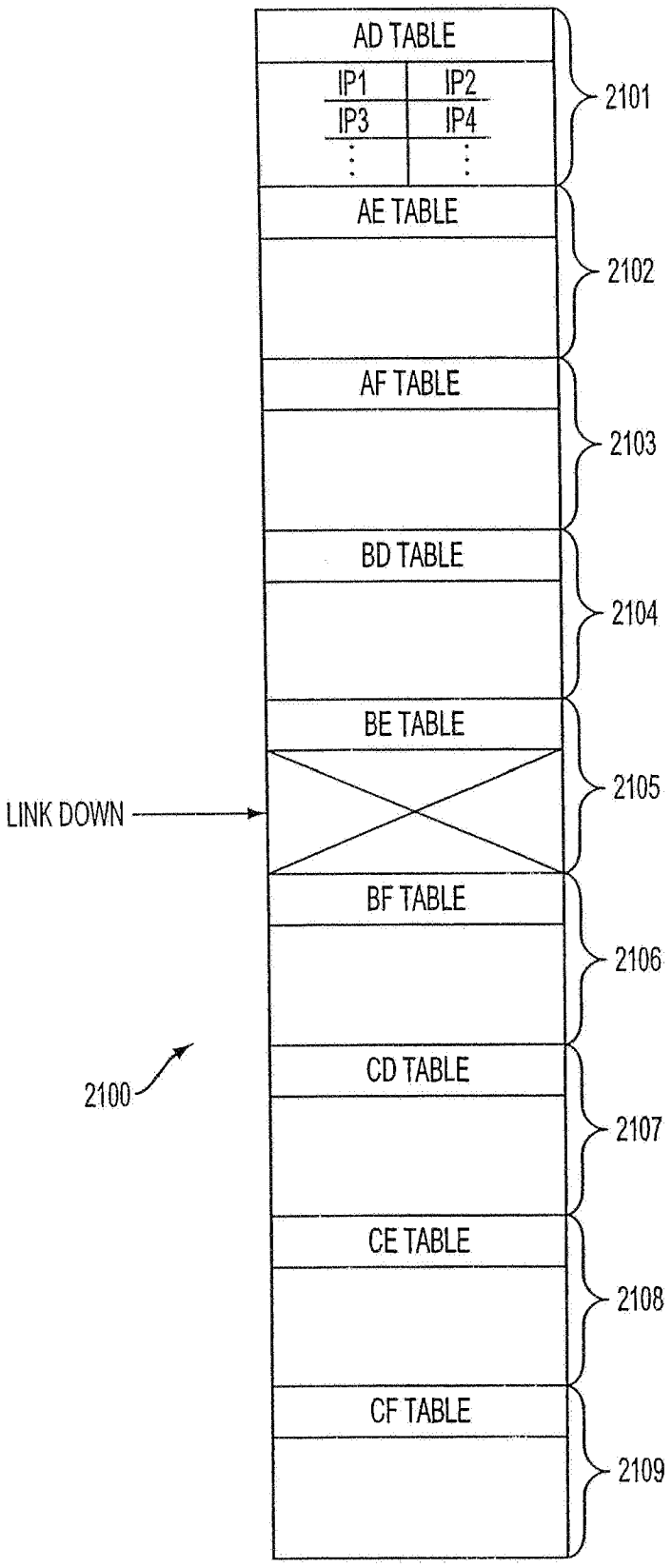

AD TABLE
IP1
IP2
IP3
IP4
2101
AE TABLE
2102
AF TABLE
2103
BD TABLE
2104
BE TABLE
2105
LINK DOWN
BF TABLE
2106
2100
CD TABLE
2107
CE TABLE
2108
CF TABLE
2109

FIG. 21

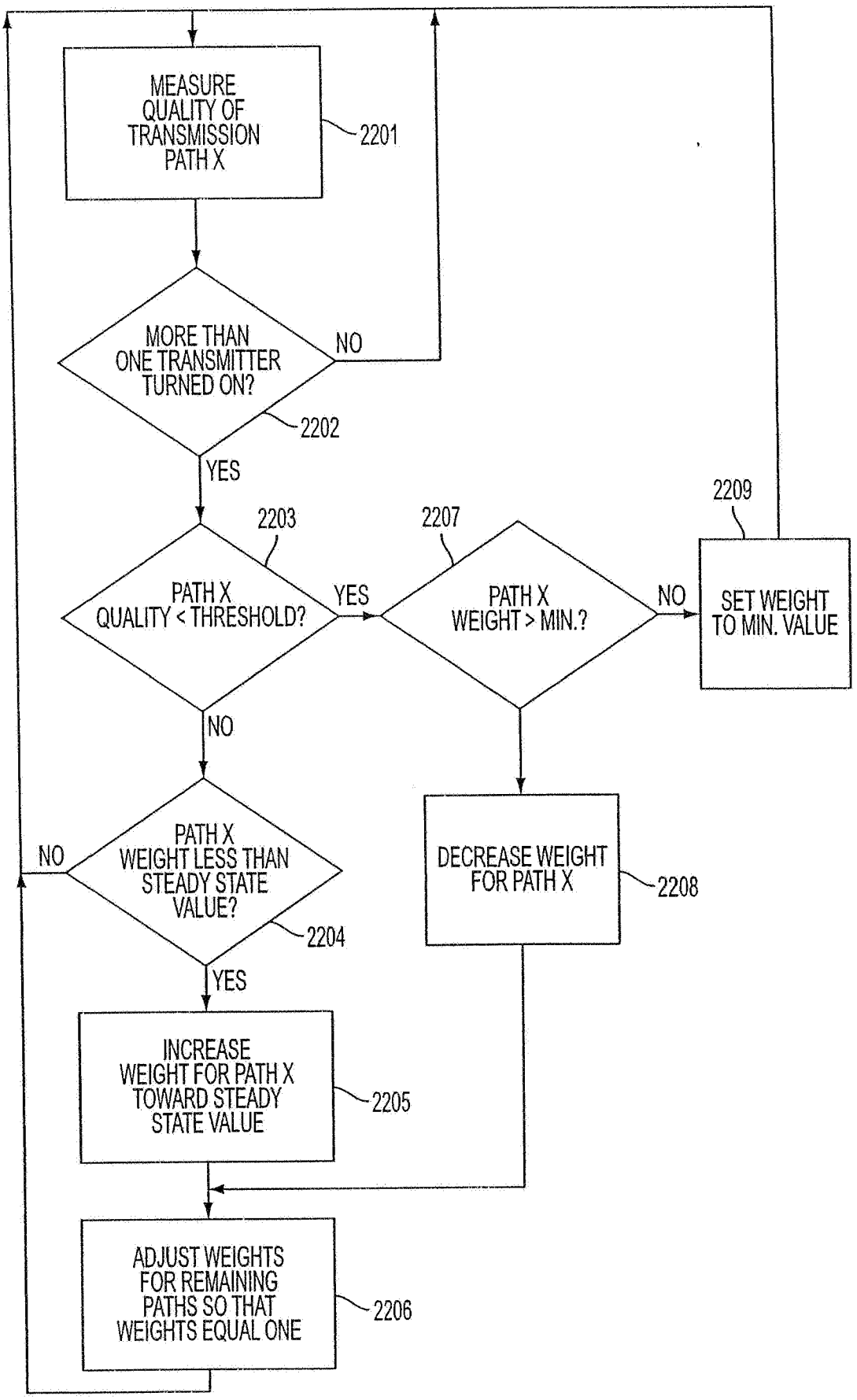

MEASURE QUALITY OF TRANSMISSION PATH X
2201
MORE THAN ONE TRANSMITTER TURNED ON?
NO
2202
YES
2203
PATH X QUALITY < THRESHOLD?
YES
2207
PATH X WEIGHT > MIN.?
NO
2209
SET WEIGHT TO MIN. VALUE
NO
PATH X WEIGHT LESS THAN STEADY STATE VALUE?
NO
2204
YES
DECREASE WEIGHT FOR PATH X
2208
INCREASE WEIGHT FOR PATH X TOWARD STEADY STATE VALUE
2205
ADJUST WEIGHTS FOR REMAINING PATHS SO THAT WEIGHTS EQUAL ONE
2206

FIG. 22A

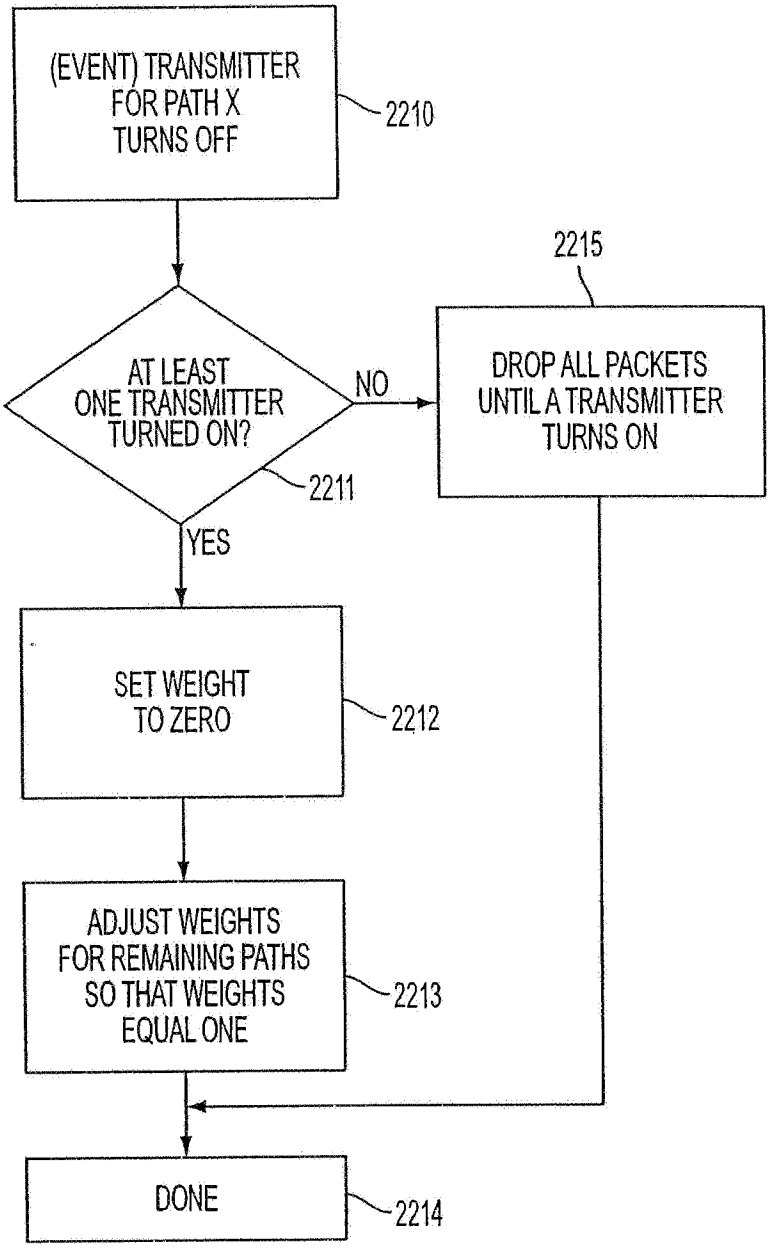

(EVENT) TRANSMITTER FOR PATH X TURNS OFF
2210
AT LEAST ONE TRANSMITTER TURNED ON?
2211
NO
2215
DROP ALL PACKETS UNTIL A TRANSMITTER TURNS ON
YES
SET WEIGHT TO ZERO
2212
ADJUST WEIGHTS FOR REMAINING PATHS SO THAT WEIGHTS EQUAL ONE
2213
DONE
2214

FIG. 22B

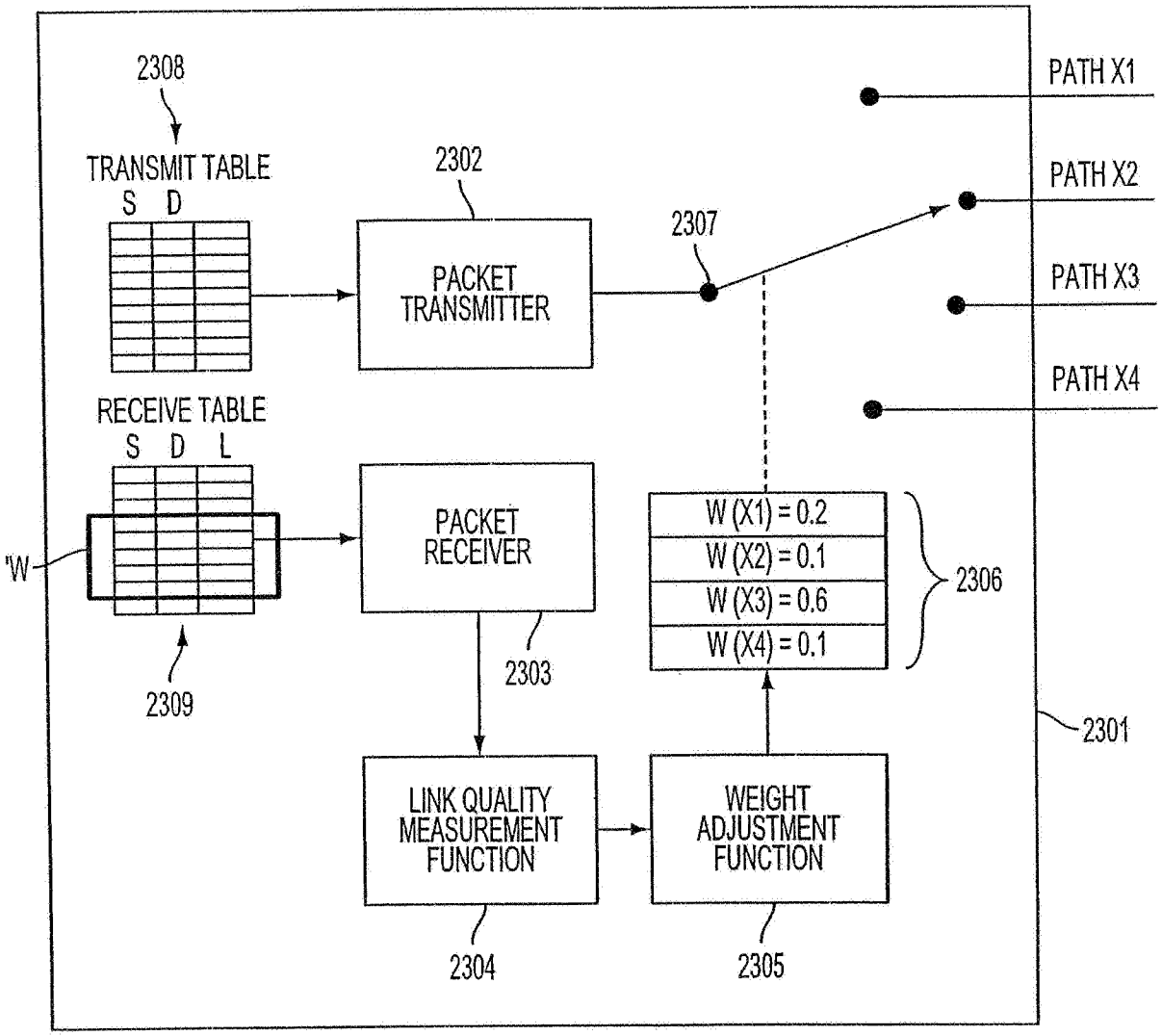

2308
TRANSMIT TABLE
S D
2302
PACKET TRANSMITTER
2307
PATH X1
PATH X2
PATH X3
PATH X4
RECEIVE TABLE
S D L
'W
PACKET RECEIVER
W (X1) = 0.2
W (X2) = 0.1
W (X3) = 0.6
W (X4) = 0.1
2306
2309
2303
2301
LINK QUALITY MEASUREMENT FUNCTION
WEIGHT ADJUSTMENT FUNCTION
2304
2305

FIG. 23

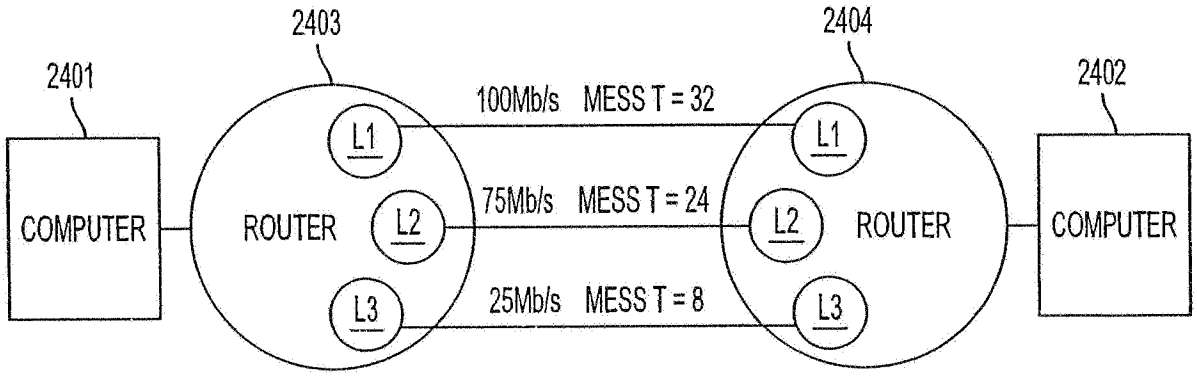

2401
2403
2404
2402
COMPUTER
ROUTER
L1
L2
L3
100Mb/s MESS T = 32
75Mb/s MESS T = 24
25Mb/s MESS T = 8
L1
L2
L3
ROUTER
COMPUTER

FIG. 24

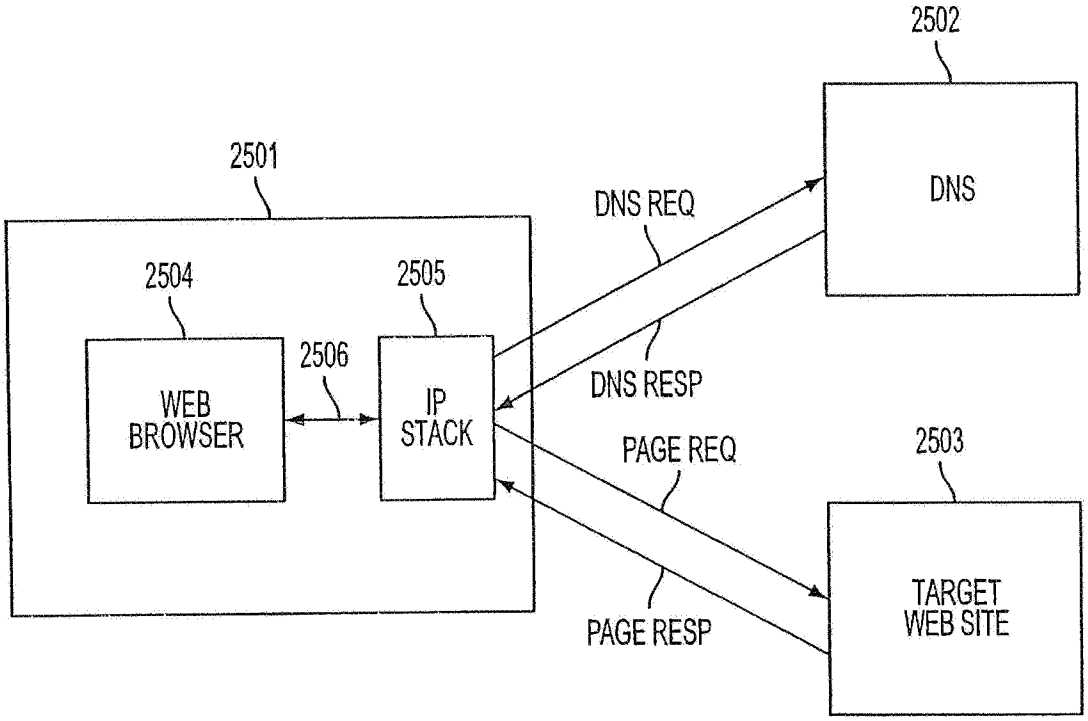


FIG. 25
(PRIOR ART)

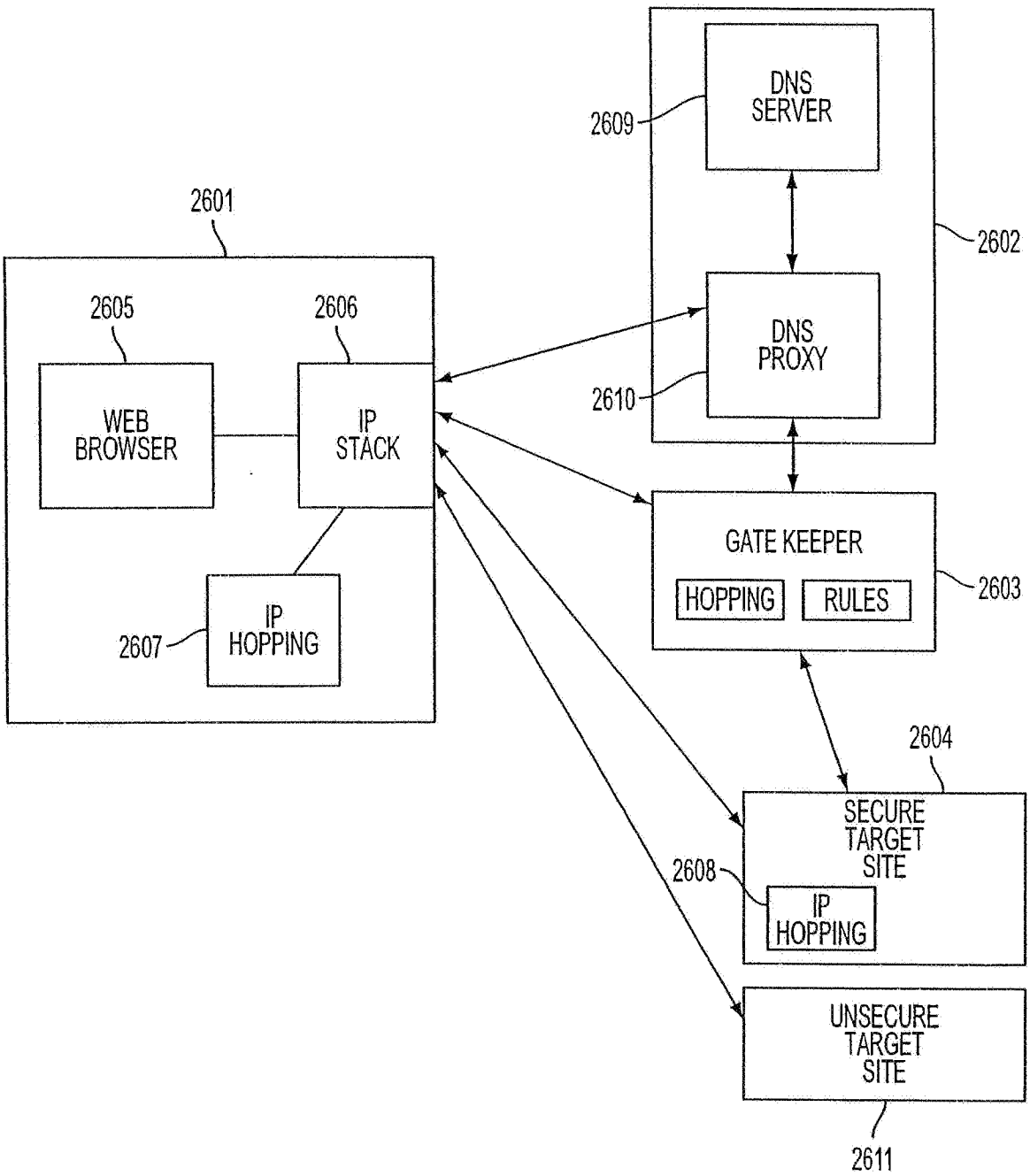

DNS SERVER
2609
2602
2601
2605
2606
DNS PROXY
WEB BROWSER
IP STACK
2610
GATE KEEPER
HOPPING
RULES
2603
IP HOPPING
2607
2604
SECURE TARGET SITE
2608
IP HOPPING
UNSECURE TARGET SITE
2611

FIG. 26

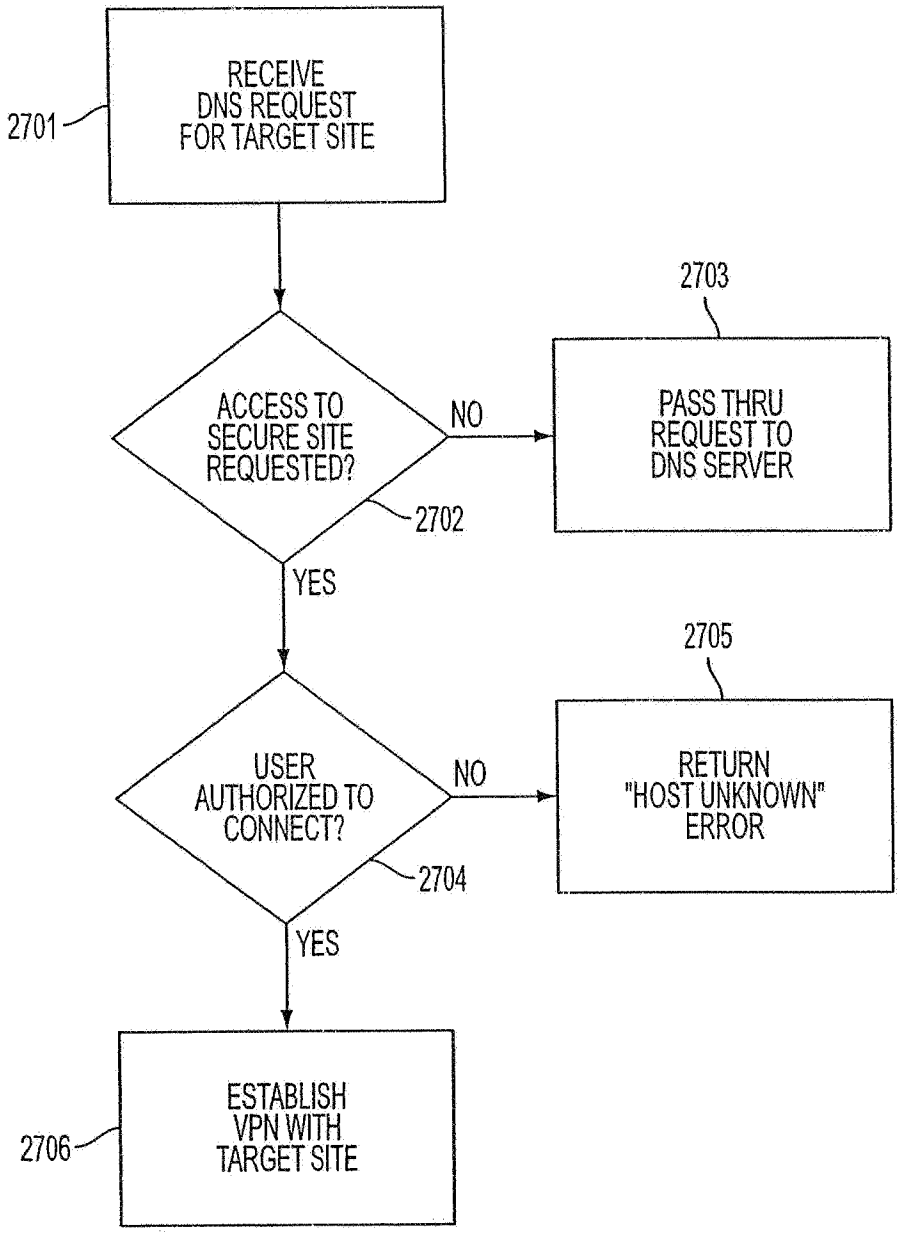

RECEIVE DNS REQUEST FOR TARGET SITE
2701
ACCESS TO SECURE SITE REQUESTED?
NO
2703
PASS THRU REQUEST TO DNS SERVER
2702
YES
USER AUTHORIZED TO CONNECT?
NO
2705
RETURN "HOST UNKNOWN" ERROR
2704
YES
ESTABLISH VPN WITH TARGET SITE
2706

FIG. 27

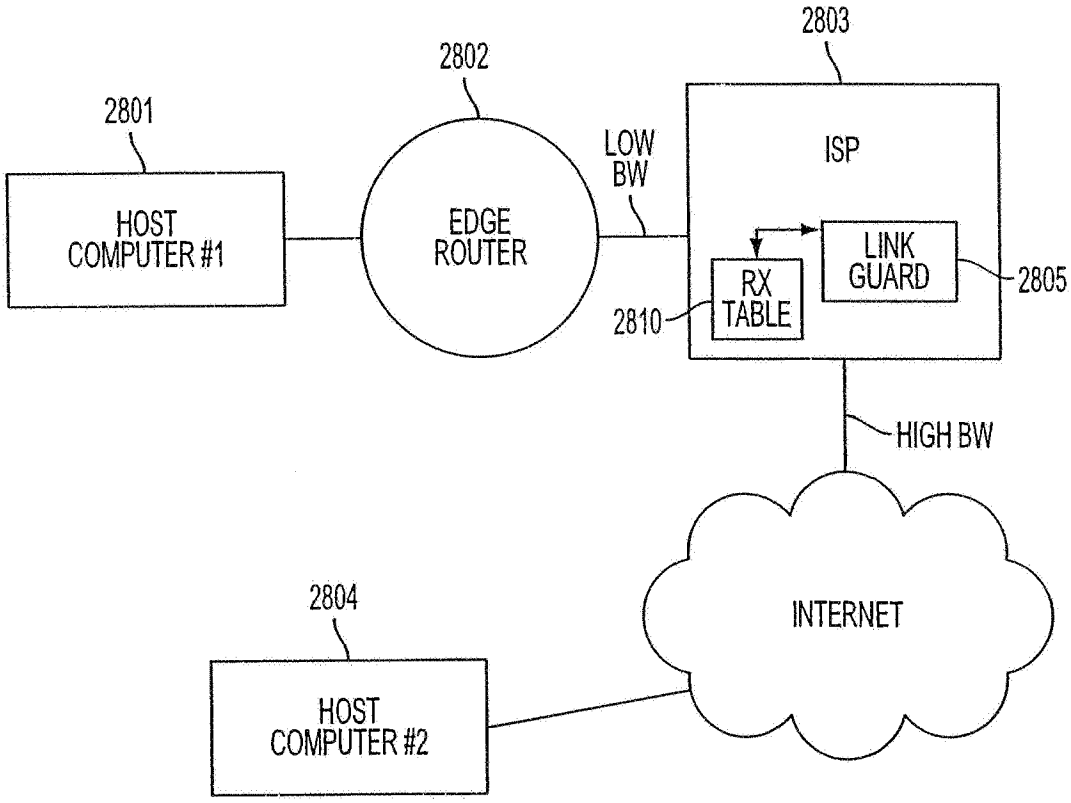

2803
2802
2801
ISP
LOW
BW
HOST
COMPUTER #1
EDGE
ROUTER
LINK
GUARD
2805
RX
TABLE
2810
HIGH BW
INTERNET
2804
HOST
COMPUTER #2

FIG. 28

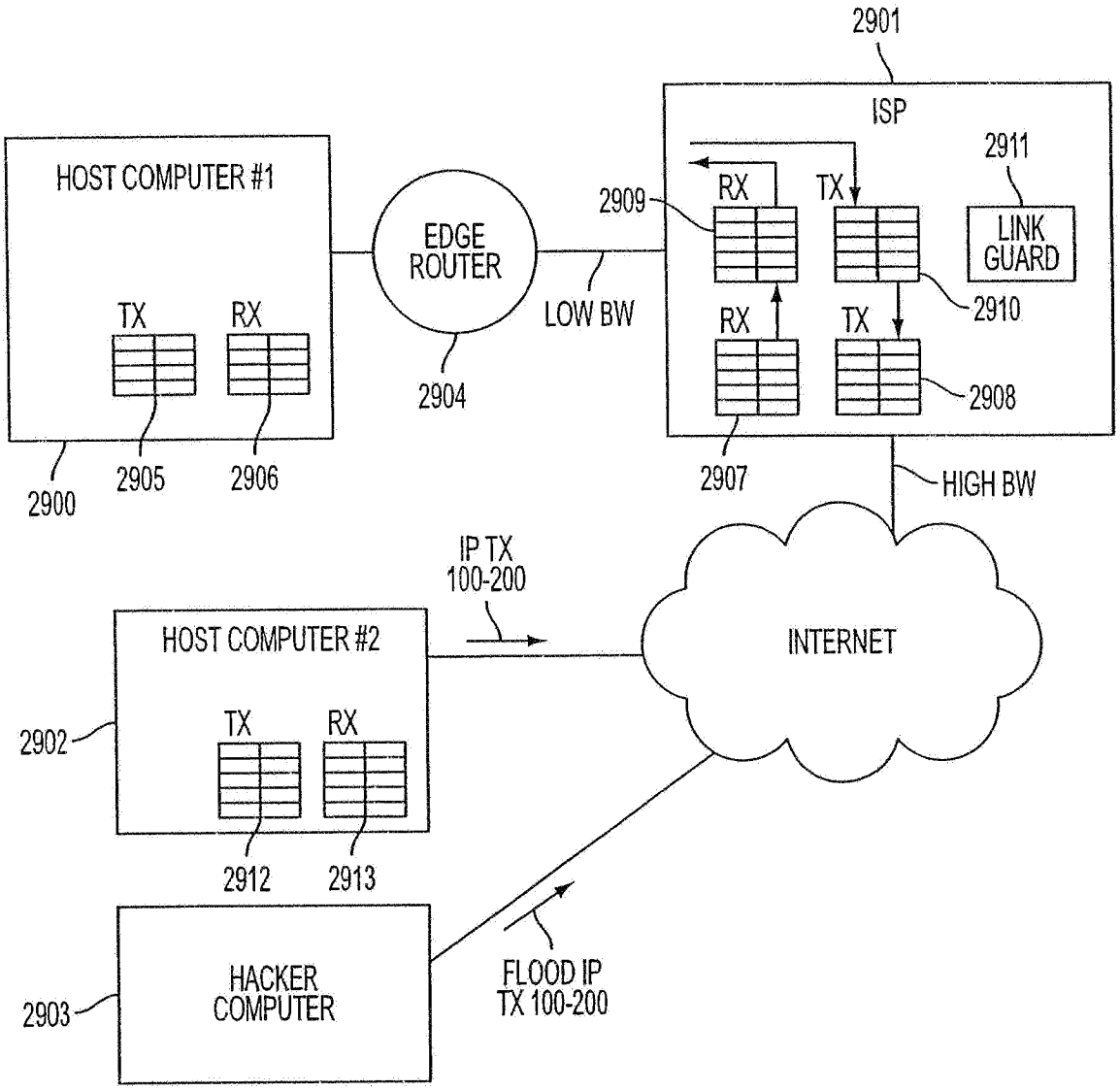

2901
ISP
HOST COMPUTER #1
EDGE ROUTER
2909
RX
TX
2911
LINK GUARD
2910
LOW BW
TX
RX
2904
RX
TX
2908
2900
2905
2906
2907
HIGH BW
IP TX 100-200
INTERNET
HOST COMPUTER #2
2902
TX
RX
2912
2913
HACKER COMPUTER
2903
FLOOD IP TX 100-200

FIG. 29

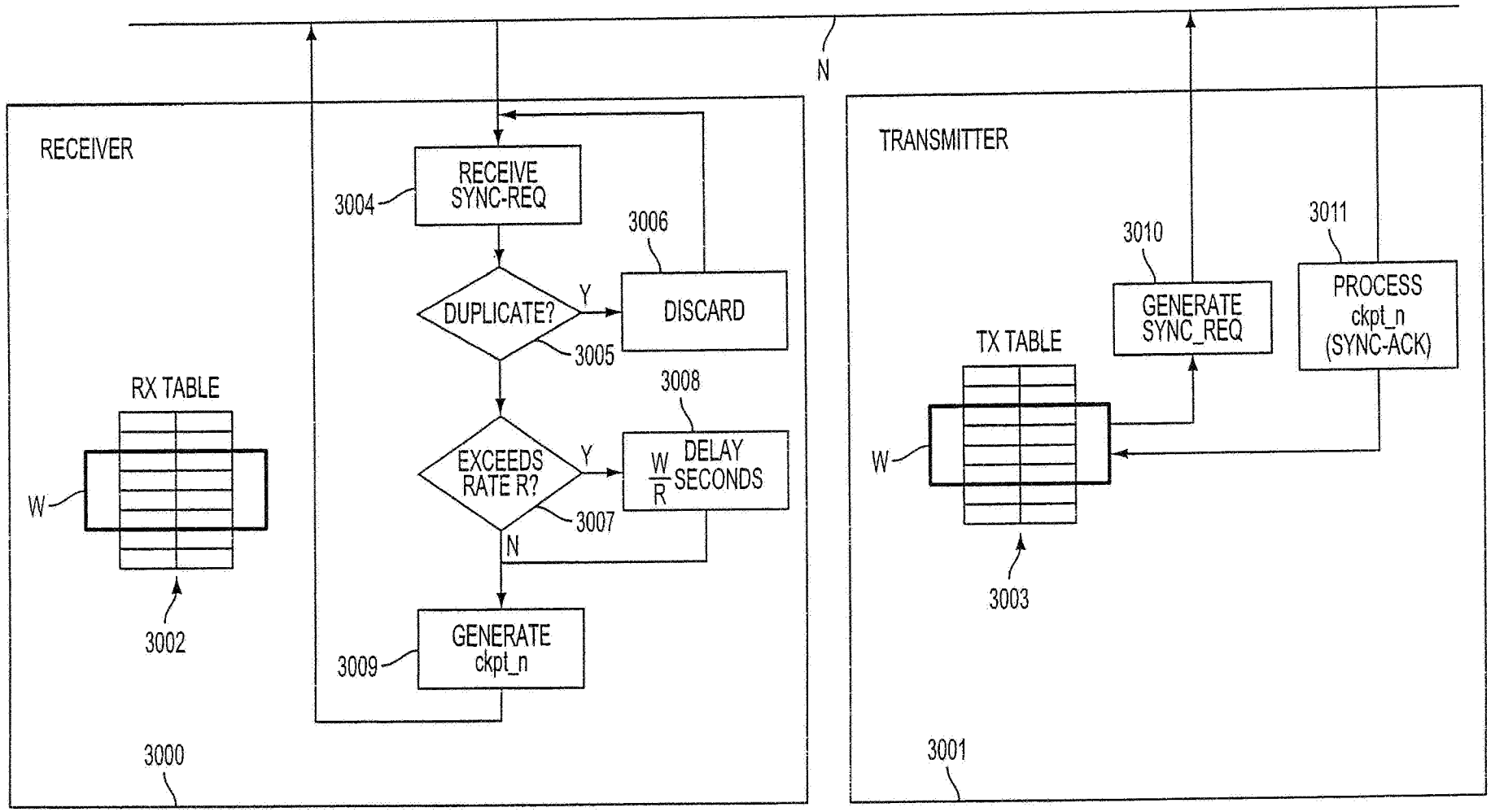


FIG. 30

Petitioner Apple Inc. - Exhibit 1002, p. 131

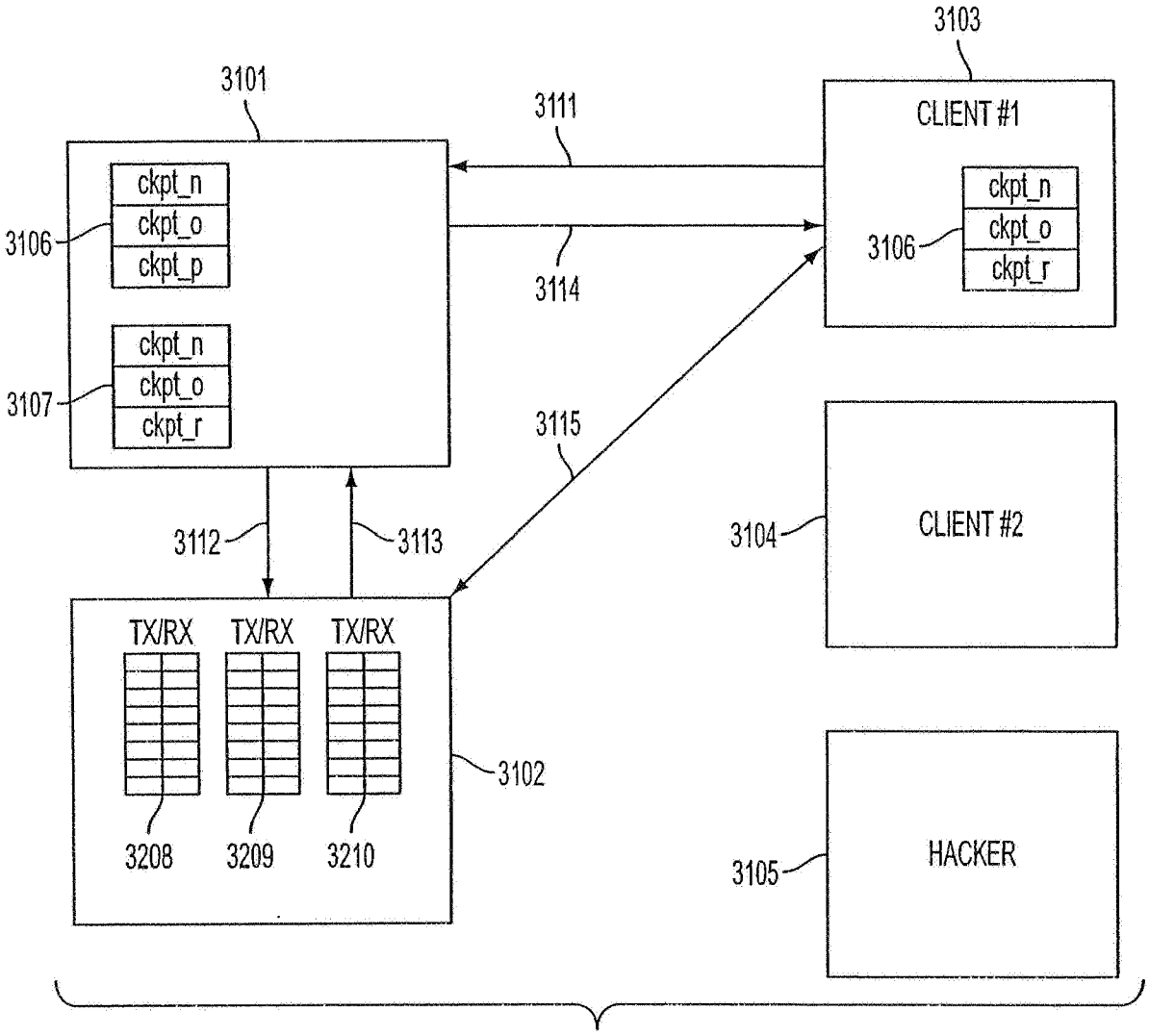

3103
3101
3111
CLIENT #1
ckpt_n
ckpt_o
ckpt_p
3106
ckpt_n
ckpt_o
ckpt_r
3106
3114
ckpt_n
ckpt_o
ckpt_r
3107
3115
3112
3113
3104
CLIENT #2
TX/RX
TX/RX
TX/RX
3102
3208
3209
3210
3105
HACKER

FIG. 31

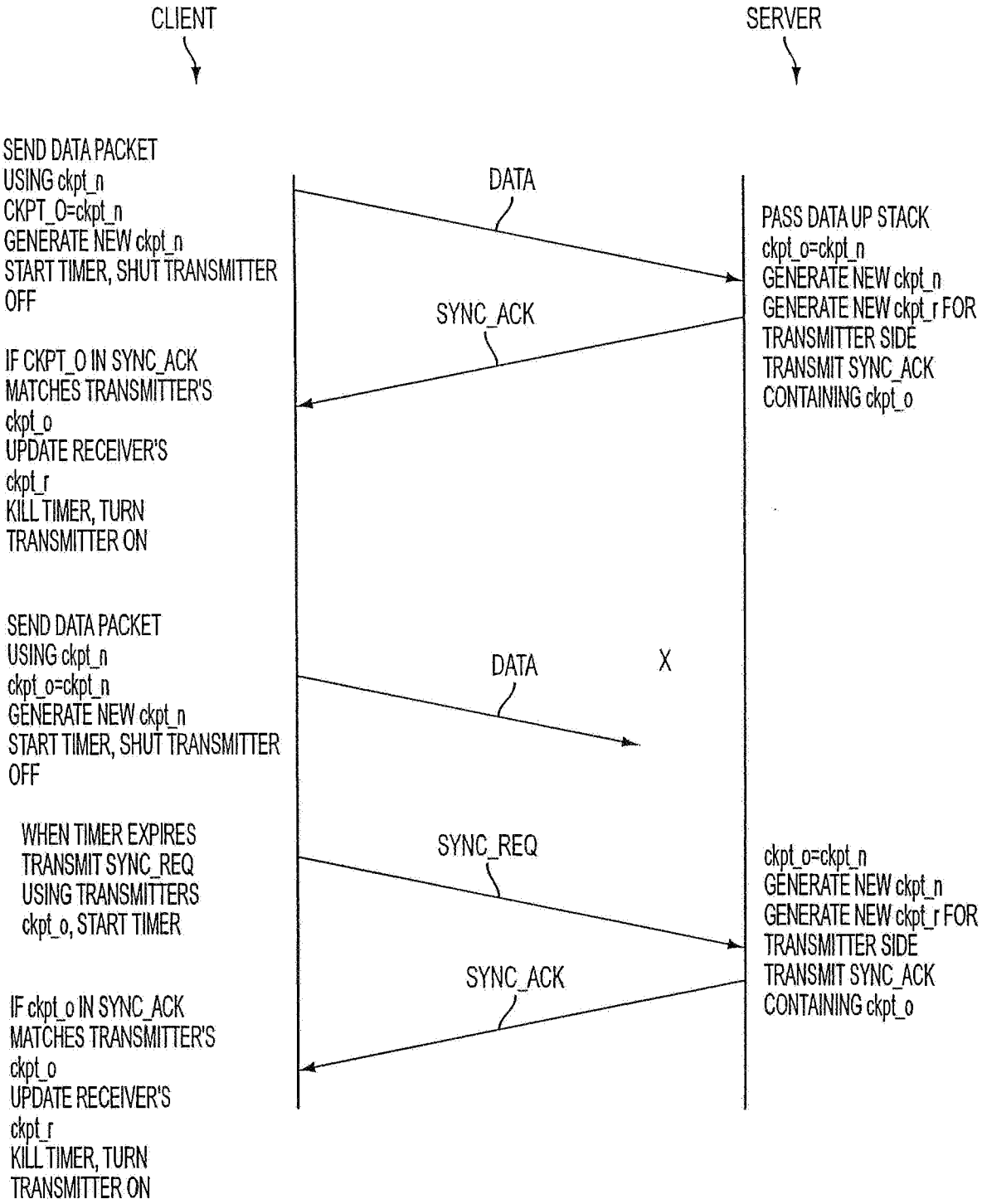

CLIENT
SERVER
SEND DATA PACKET
USING ckpt_n
CKPT_O=ckpt_n
GENERATE NEW ckpt_n
START TIMER, SHUT TRANSMITTER OFF
DATA
PASS DATA UP STACK
ckpt_o=ckpt_n
GENERATE NEW ckpt_n
GENERATE NEW ckpt_r FOR TRANSMITTER SIDE
TRANSMIT SYNC_ACK CONTAINING ckpt_o
SYNC_ACK
IF CKPT_O IN SYNC_ACK MATCHES TRANSMITTER'S ckpt_o
UPDATE RECEIVER'S ckpt_r
KILL TIMER, TURN TRANSMITTER ON
SEND DATA PACKET
USING ckpt_n
ckpt_o=ckpt_n
GENERATE NEW ckpt_n
START TIMER, SHUT TRANSMITTER OFF
DATA
X
WHEN TIMER EXPIRES
TRANSMIT SYNC_REQ
USING TRANSMITTERS
ckpt_o, START TIMER
SYNC_REQ
ckpt_o=ckpt_n
GENERATE NEW ckpt_n
GENERATE NEW ckpt_r FOR TRANSMITTER SIDE
TRANSMIT SYNC_ACK CONTAINING ckpt_o
SYNC_ACK
IF ckpt_o IN SYNC_ACK MATCHES TRANSMITTER'S ckpt_o
UPDATE RECEIVER'S ckpt_r
KILL TIMER, TURN TRANSMITTER ON

FIG. 32

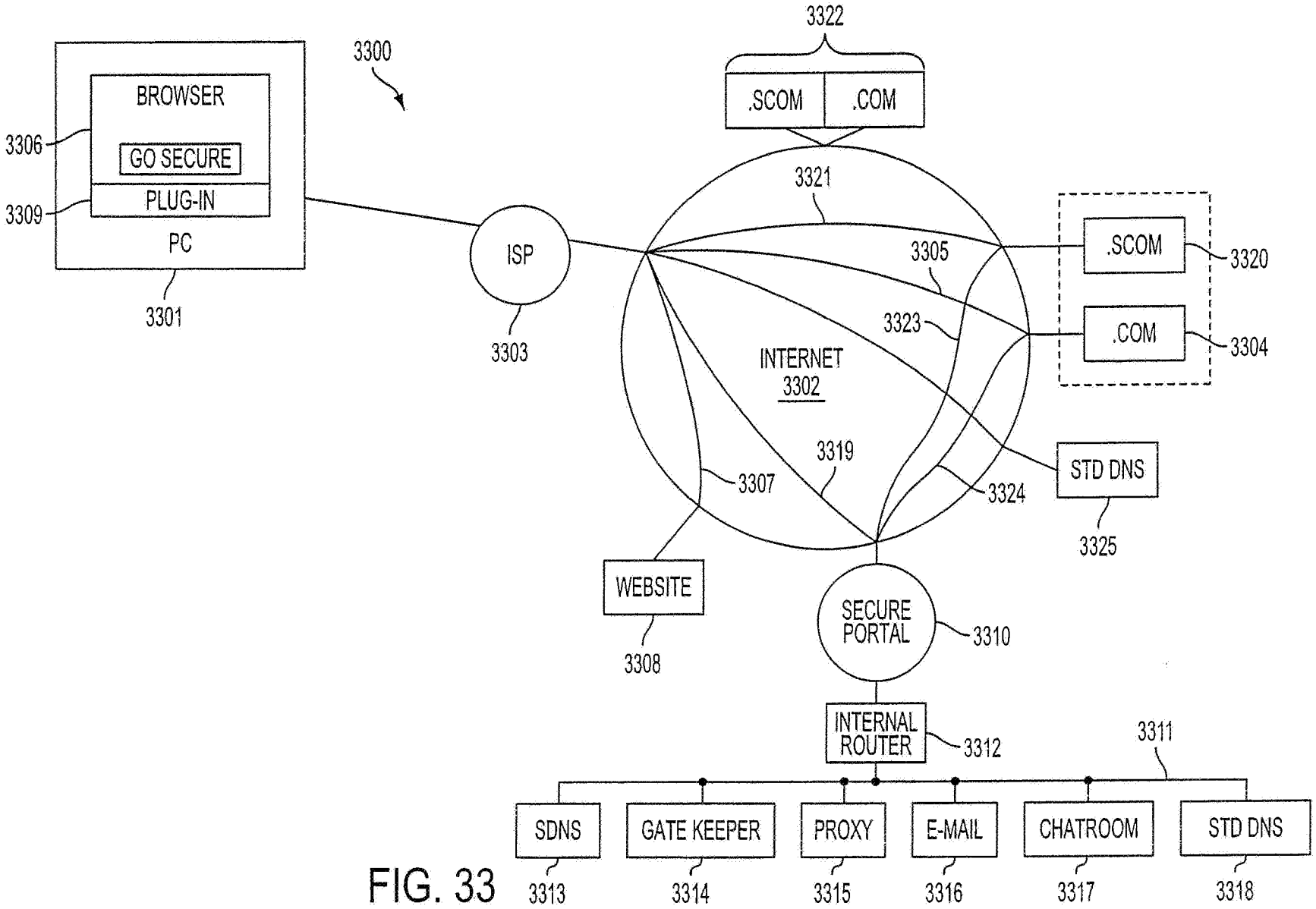


FIG. 33

Petitioner Apple Inc. - Exhibit 1002, p. 134

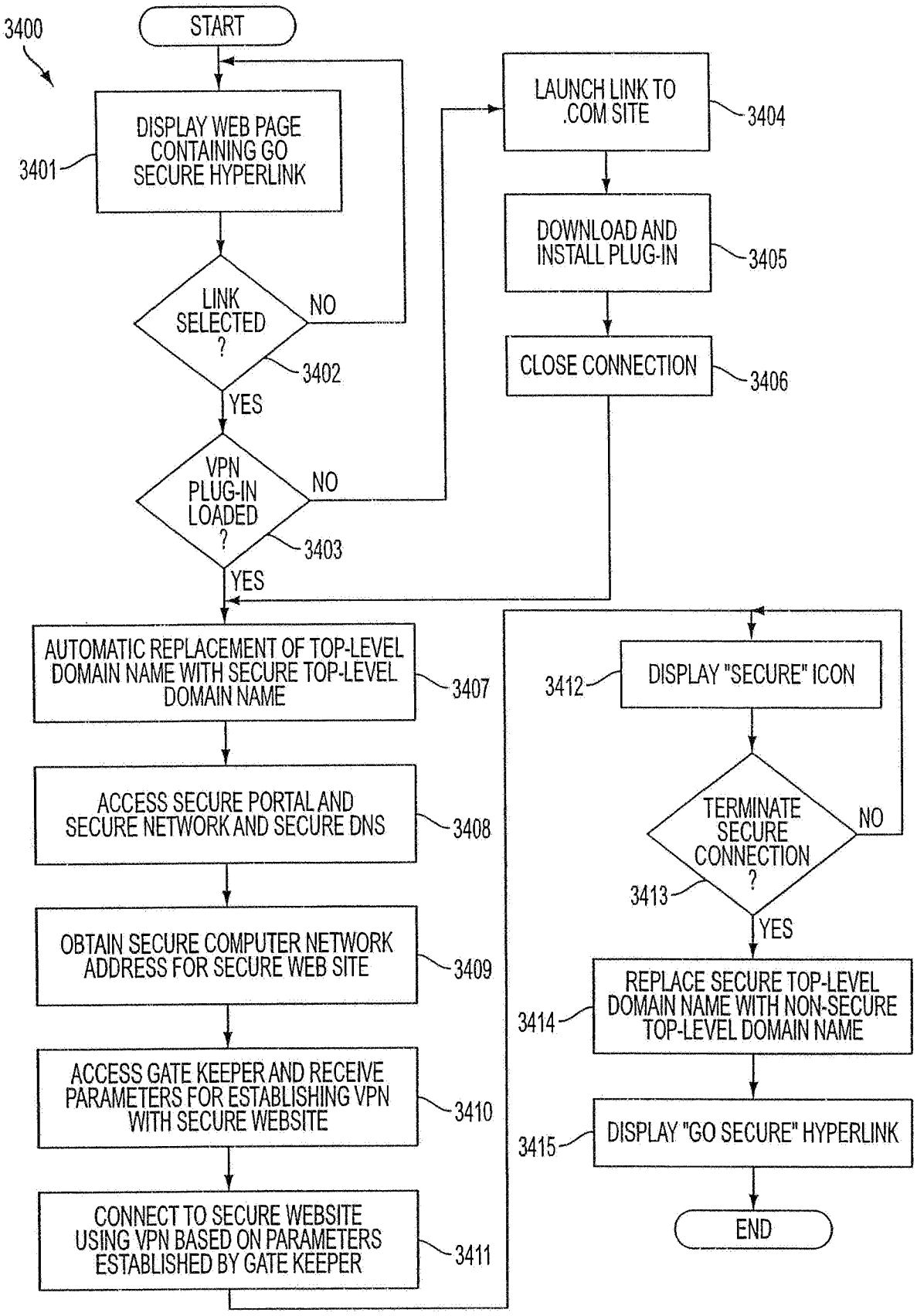

3400
START
DISPLAY WEB PAGE CONTAINING GO SECURE HYPERLINK
3401
LINK SELECTED ?
NO
3402
YES
VPN PLUG-IN LOADED ?
NO
3403
YES
LAUNCH LINK TO .COM SITE
3404
DOWNLOAD AND INSTALL PLUG-IN
3405
CLOSE CONNECTION
3406
AUTOMATIC REPLACEMENT OF TOP-LEVEL DOMAIN NAME WITH SECURE TOP-LEVEL DOMAIN NAME
3407
ACCESS SECURE PORTAL AND SECURE NETWORK AND SECURE DNS
3408
OBTAIN SECURE COMPUTER NETWORK ADDRESS FOR SECURE WEB SITE
3409
ACCESS GATE KEEPER AND RECEIVE PARAMETERS FOR ESTABLISHING VPN WITH SECURE WEBSITE
3410
CONNECT TO SECURE WEBSITE USING VPN BASED ON PARAMETERS ESTABLISHED BY GATE KEEPER
3411
3412
DISPLAY "SECURE" ICON
TERMINATE SECURE CONNECTION ?
NO
3413
YES
REPLACE SECURE TOP-LEVEL DOMAIN NAME WITH NON-SECURE TOP-LEVEL DOMAIN NAME
3414
DISPLAY "GO SECURE" HYPERLINK
3415
END

FIG. 34

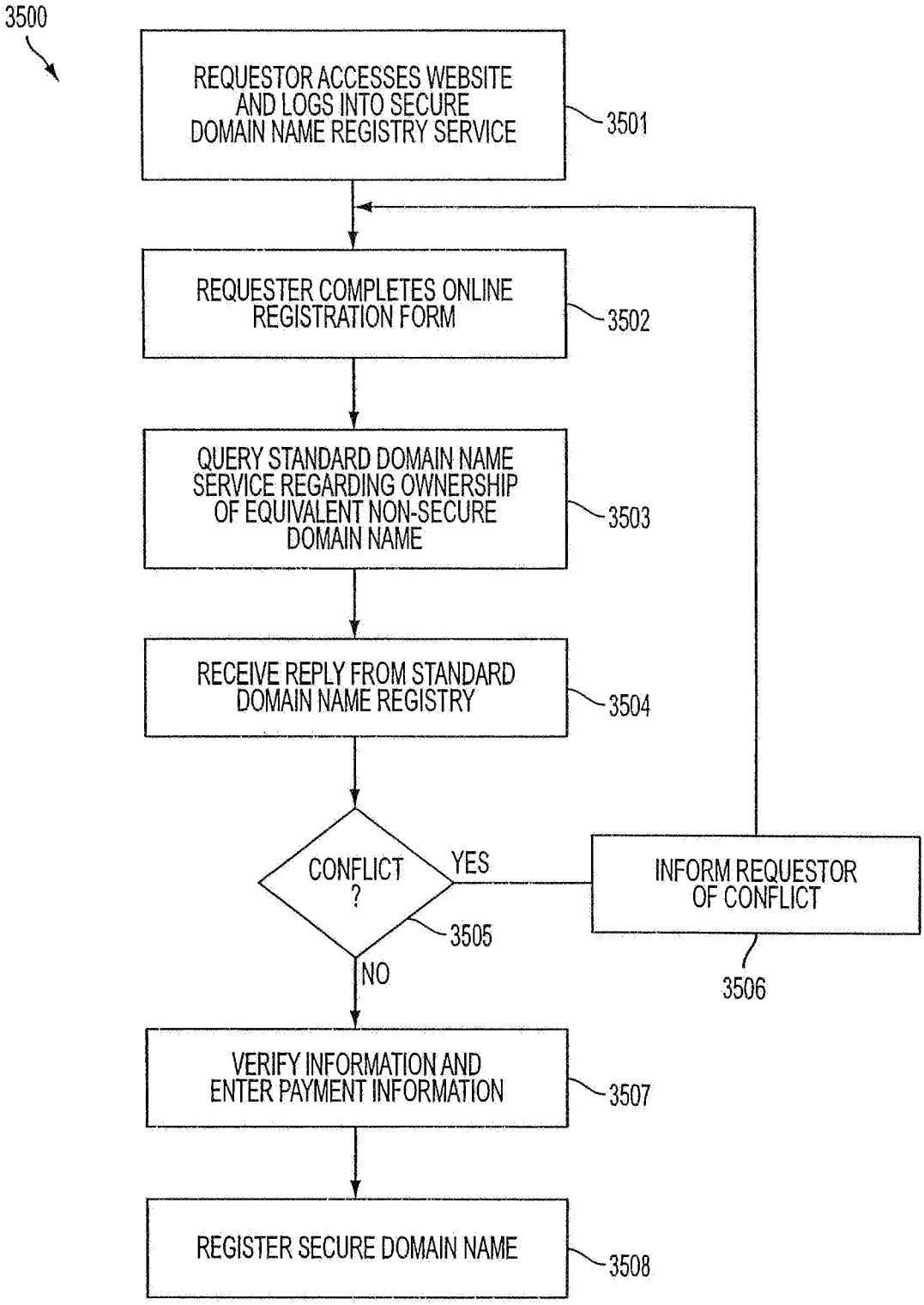

3500
REQUESTOR ACCESSES WEBSITE AND LOGS INTO SECURE DOMAIN NAME REGISTRY SERVICE
3501
REQUESTER COMPLETES ONLINE REGISTRATION FORM
3502
QUERY STANDARD DOMAIN NAME SERVICE REGARDING OWNERSHIP OF EQUIVALENT NON-SECURE DOMAIN NAME
3503
RECEIVE REPLY FROM STANDARD DOMAIN NAME REGISTRY
3504
CONFLICT ?
YES
3505
NO
INFORM REQUESTOR OF CONFLICT
3506
VERIFY INFORMATION AND ENTER PAYMENT INFORMATION
3507
REGISTER SECURE DOMAIN NAME
3508

FIG. 35

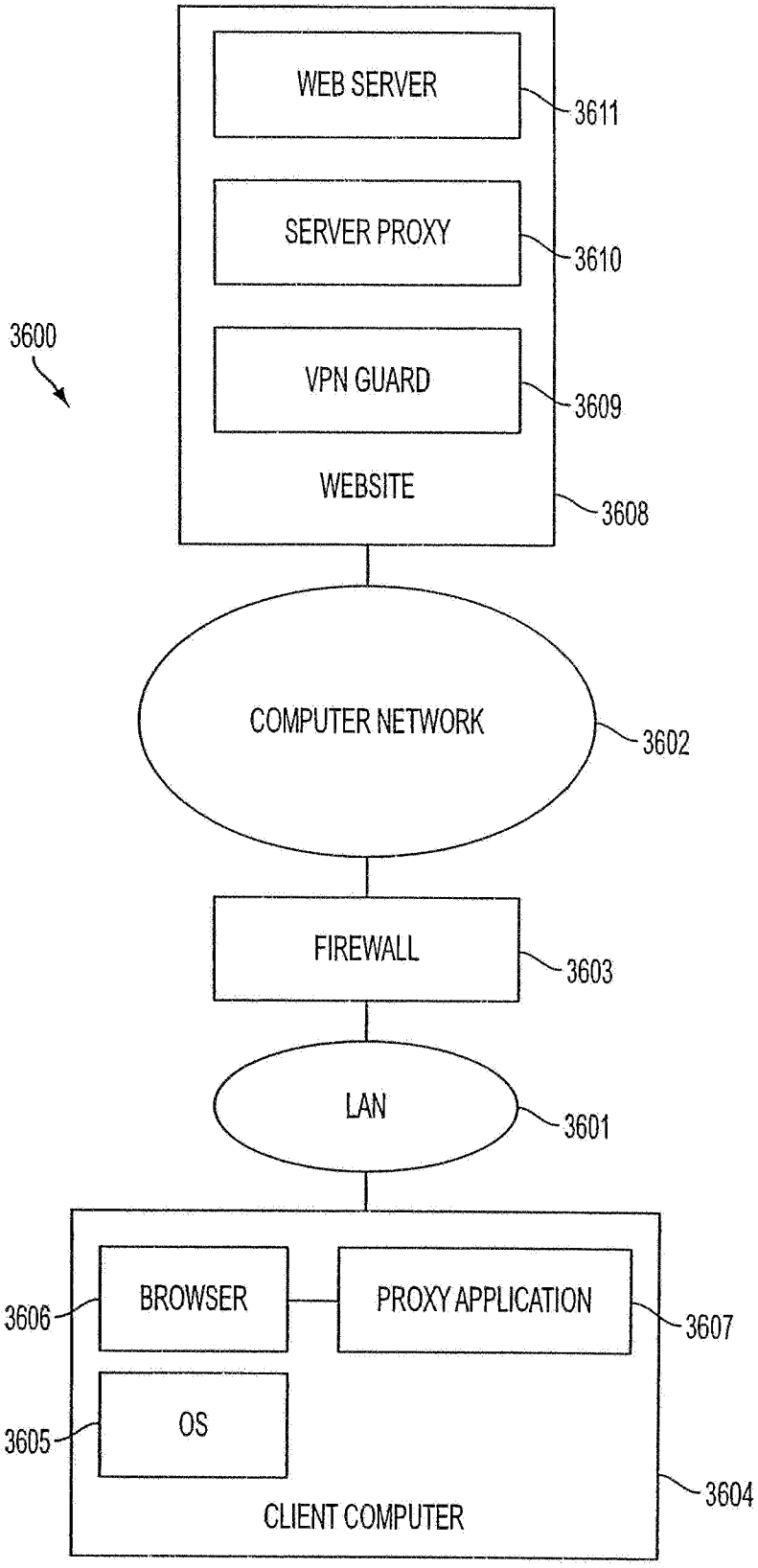

3600
WEB SERVER
3611
SERVER PROXY
3610
VPN GUARD
3609
WEBSITE
3608
COMPUTER NETWORK
3602
FIREWALL
3603
LAN
3601
BROWSER
3606
PROXY APPLICATION
3607
OS
3605
CLIENT COMPUTER
3604

FIG. 36

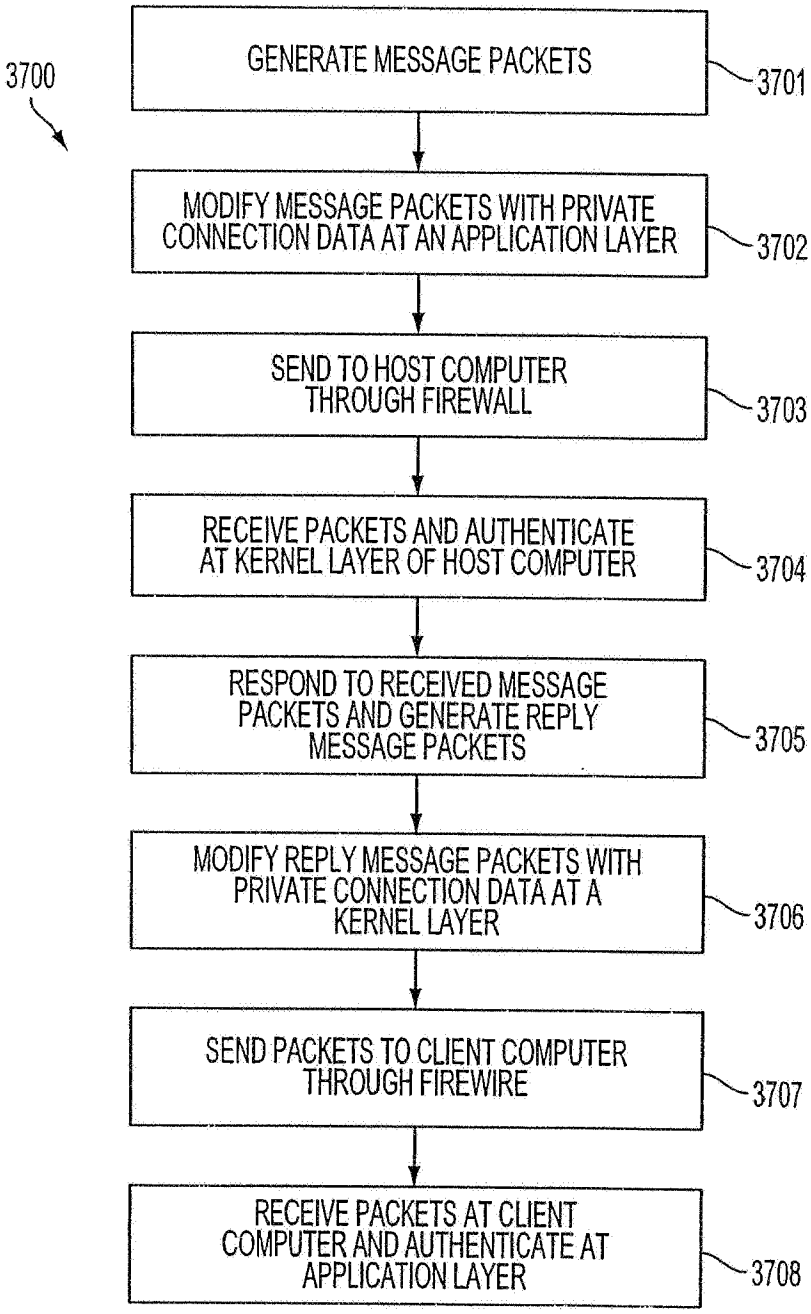

3700
GENERATE MESSAGE PACKETS
3701
MODIFY MESSAGE PACKETS WITH PRIVATE CONNECTION DATA AT AN APPLICATION LAYER
3702
SEND TO HOST COMPUTER THROUGH FIREWALL
3703
RECEIVE PACKETS AND AUTHENTICATE AT KERNEL LAYER OF HOST COMPUTER
3704
RESPOND TO RECEIVED MESSAGE PACKETS AND GENERATE REPLY MESSAGE PACKETS
3705
MODIFY REPLY MESSAGE PACKETS WITH PRIVATE CONNECTION DATA AT A KERNEL LAYER
3706
SEND PACKETS TO CLIENT COMPUTER THROUGH FIREWIRE
3707
RECEIVE PACKETS AT CLIENT COMPUTER AND AUTHENTICATE AT APPLICATION LAYER
3708

FIG. 37

PTO/SB/14 (11-08)
Approved for use through 09/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	77580-151(VRNK-1CP3CNFT1)
	Application Number	
Title of Invention	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Applicant Information:

Applicant 1 Remove

Applicant Authority ◉ Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Victor		Larson	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Fairfax	State/Province	VA	Country of Residence[i]	US

Citizenship under 37 CFR 1.41(b)[i] US

Mailing Address of Applicant:

Address 1	12026 Lisa Marie Court		
Address 2			
City	Fairfax	State/Province	VA
Postal Code	22033	Country[i]	US

Applicant 2 Remove

Applicant Authority ◉ Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Robert	Dunham	Short	III

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Leesburg	State/Province	VA	Country of Residence[i]	US

Citizenship under 37 CFR 1.41(b)[i] US

Mailing Address of Applicant:

Address 1	38710 Goose Creek Lane		
Address 2			
City	Leesburg	State/Province	VA
Postal Code	20175	Country[i]	US

Applicant 3 Remove

Applicant Authority ◉ Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Edmond	Colby	Munger	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Crownsville	State/Province	MD	Country of Residence[i]	US

PTO/SB/14 (11-08)
Approved for use through 09/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	77580-151(VRNK-1CP3CNFT1)
	Application Number	
Title of Invention	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES	

Citizenship under 37 CFR 1.41(b) i	US				
Mailing Address of Applicant:					
Address 1	1101 Opaca Court				
Address 2					
City	Crownsville	**State/Province**	MD		
Postal Code	21032	**Country**i	US		

Applicant 4 Remove

Applicant Authority (•) Inventor ( ) Legal Representative under 35 U.S.C. 117 ( ) Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Michael		Williamson	

Residence Information (Select One) (•) US Residency ( ) Non US Residency ( ) Active US Military Service

City	South Riding	**State/Province**	VA	**Country of Residence** i	US
Citizenship under 37 CFR 1.41(b) i	US				
Mailing Address of Applicant:					
Address 1	26203 Ocala Circle				
Address 2					
City	South Riding	**State/Province**	VA		
Postal Code	20152	**Country**i	US		

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	23630		
Email Address	mweipdocket@mwe.com	Add Email	Remove Email

Application Information:

Title of the Invention	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES		
Attorney Docket Number	77580-151(VRNK-1CP3CNFT1)	**Small Entity Status Claimed**	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)	707	**Sub Class (if any)**	770
Suggested Technology Center (if any)	2100		
Total Number of Drawing Sheets (if any)	40	**Suggested Figure for Publication (if any)**	

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	77580-151(VRNK-1CP3CNFT1)
	Application Number	
Title of Invention	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES	

Publication Information:

☐	Request Early Publication (Fee required at time of Request 37 CFR 1.219)
☐	**Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S. C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Enter either Customer Number or complete the Representative Name section below. If both sections are completed the Customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	23630		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	13/049552	2011-03-16

Prior Application Status	Patented		Remove		
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13/049552	Continuation of	11/840560	2007-08-17	7921211	2011-04-05

Prior Application Status	Patented		Remove		
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
11/840560	Continuation of	10/714849	2003-11-18	7418504	2008-08-26

Prior Application Status	Abandoned		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
10/714849	Continuation of	09/558210	2000-04-26

Prior Application Status	Patented		Remove		
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
09/558210	Continuation in part of	09/504783	2000-02-15	6502135	2002-12-31

Prior Application Status	Patented		Remove

PTO/SB/14 (11-08)
Approved for use through 09/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	77580-151(VRNK-1CP3CNFT1)
	Application Number	
Title of Invention	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES	

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
09/504783	Continuation in part of	09/429643	1999-10-29	7010604	2006-03-07

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
09/429643	non provisional of	60/106261	1998-10-30
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
09/429643	non provisional of	60/137704	1999-06-07

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).

Remove

Application Number	Country [i]	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
			(•) Yes ( ) No

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Assignee Information:

Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office.

Assignee 1 Remove

If the Assignee is an Organization check here.	☒		
Organization Name	VIRNETX, INC.		
Mailing Address Information:			
Address 1	5615 Scotts Valley Drive, Suite 110		
Address 2			
City	Scotts Valley	**State/Province**	CA
Country [i] US		Postal Code	95066
Phone Number	--	Fax Number	--
Email Address	--		

Additional Assignee Data may be generated within this form by selecting the **Add** button. Add

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.

PTO/SB/14 (11-08)
Approved for use through 09/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	77580-151(VRNK-1CP3CNFT1)
	Application Number	
Title of Invention	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES	

Signature	/Toby H. Kusmer/			Date (YYYY-MM-DD)	2011-12-23
First Name	Toby H.	Last Name	Kusmer, P.C.	Registration Number	26418

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Petitioner Apple Inc. - Exhibit 1002, p. 144

JOINT DECLARATION FOR PATENT APPLICATION

As the below named inventors, we hereby declare that:

Our residence, post office address and citizenship are as stated below next to our names;

We believe we are the original, first and joint inventors of the subject matter which is claimed and for which a patent is sought on the invention entitled AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES, the specification of which

- ☒ is attached hereto.
- ☐ was filed on _____as Application Serial Number _____and was amended on _____ (if applicable).
- ☐ was filed under the Patent Cooperation Treaty (PCT) and accorded International Application No. _____, filed _____, and amended on _____ (if any).

We hereby state that we have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

We hereby acknowledge the duty to disclose information which is material to patentability in accordance with Title 37, Code of Federal Regulations, §1.56(a).

Prior Foreign Application(s)

We hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application(s) for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Country	Application No.	Date of Filing (day, month, year)	Date of Issue (day, month, year)	Priority Claimed Under 35 U.S.C. §119

Prior United States Provisional Application(s)

We hereby claim priority benefits under Title 35, United States Code, §119(e)(1) of any U.S. provisional application listed below:

U.S. Provisional Application No.	Date of Filing (day, month, year)	Priority Claimed Under 35 U.S.C. §119(e)(1)
60/106,261	30 October 1998	Yes
60/137,704	7 June 1999	Yes

Prior United States Application(s)

We hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, we acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Petitioner Apple Inc. - Exhibit 1002, p. 145

Application Serial No.	Date of Filing (Day, Month, Year)	Status — Patented, Pending, Abandoned
09/558,210	26 April 2000	Pending
09/504,783	15 February 2000	Patented
09/429,643	29 October 1999	Pending

Power of Attorney

And we hereby appoint, both jointly and severally, as our attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith the practitioners at:

Customer Number: 22907 (WDC)

Please address all correspondence and telephone communications to the address and telephone number for this Customer Number.

We hereby declare that all statements made herein of our own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Signature Victor Larson Date 11/10/2003
Full Name of First Inventor Larson (Family Name) Victor (First Given Name) (Second Given Name)
Residence Fairfax, Virginia Citizenship USA
Post Office Address 12026 Lisa Marie Court, Fairfax, Virginia 22033

Signature _____ Date _____
Full Name of Second Inventor Short, III (Family Name) Robert (First Given Name) Dunham (Second Given Name)
Residence Leesburg, Virginia Citizenship USA
Post Office Address 38710 Goose Creek Lane, Leesburg, Virginia 20175

Signature _____ Date _____
Full Name of Third Inventor Munger (Family Name) Edmund (First Given Name) Colby (Second Given Name)
Residence Crownsville, Maryland Citizenship USA
Post Office Address 1101 Opaca Court, Crownsville, Maryland 21032

Signature _____ Date Nov 10 2003
Full Name of Fourth Inventor Williamson (Family Name) Michael (First Given Name) (Second Given Name)
Residence South Riding, Virginia Citizenship USA
Post Office Address 26203 Ocala Circle, South Riding, Virginia 20152

Petitioner Apple Inc. - Exhibit 1002, p. 146

JOINT DECLARATION FOR PATENT APPLICATION

As the below named inventors, we hereby declare that:

Our residence, post office address and citizenship are as stated below next to our names;

We believe we are the original, first and joint inventors of the subject matter which is claimed and for which a patent is sought on the invention entitled AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES, the specification of which

- ☒ is attached hereto.
- ☐ was filed on _____as Application Serial Number _____and was amended on _____ (if applicable).
- ☐ was filed under the Patent Cooperation Treaty (PCT) and accorded International Application No. _____, filed _____, and amended on _____ (if any).

We hereby state that we have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

We hereby acknowledge the duty to disclose information which is material to patentability in accordance with Title 37, Code of Federal Regulations, §1.56(a).

Prior Foreign Application(s)

We hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application(s) for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Country	Application Number	Date of Filing (day, month, year)	Date of Issue (day, month, year)	Priority Claimed Under 35 U.S.C. §119

Prior United States Provisional Application(s)

We hereby claim priority benefits under Title 35, United States Code, §119(e)(1) of any U.S. provisional application listed below:

U.S. Provisional Application No.	Date of Filing (day, month, year)	Priority Claimed Under 35 U.S.C. §119(e)(1)
60/106,261	30 October 1998	Yes
60/137,704	7 June 1999	Yes

Prior United States Application(s)

We hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, we acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Petitioner Apple Inc. - Exhibit 1002, p. 147

Application Serial No.	Date of Filing (Day, Month, Year)	Status — Patented, Pending, Abandoned
09/558,210	26 April 2000	Pending
09/504,783	15 February 2000	Patented
09/429,643	29 October 1999	Pending

Power of Attorney

And we hereby appoint, both jointly and severally, as our attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith the practitioners at:

Customer Number: 22907 (WDC)

Please address all correspondence and telephone communications to the address and telephone number for this Customer Number.

We hereby declare that all statements made herein of our own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Signature_____ Date_____
Full Name of First Inventor Larson (Family Name) Victor (First Given Name) (Second Given Name)
Residence Fairfax, Virginia Citizenship USA
Post Office Address 12026 Lisa Marie Court, Fairfax, Virginia 22033

Signature [signature] Date 11/7/03
Full Name of Second Inventor Short, III (Family Name) Robert (First Given Name) Dunham (Second Given Name)
Residence Leesburg, Virginia Citizenship USA
Post Office Address 38710 Goose Creek Lane, Leesburg, Virginia 20175

Signature_____ Date_____
Full Name of Third Inventor Munger (Family Name) Edmund (First Given Name) Colby (Second Given Name)
Residence Crownsville, Maryland Citizenship USA
Post Office Address 1101 Opaca Court, Crownsville, Maryland 21032

Signature_____ Date_____
Full Name of Fourth Inventor Williamson (Family Name) Michael (First Given Name) (Second Given Name)
Residence South Riding, Virginia Citizenship USA
Post Office Address 26203 Ocala Circle, South Riding, Virginia 20152

Petitioner Apple Inc. - Exhibit 1002, p. 148

JOINT DECLARATION FOR PATENT APPLICATION

As the below named inventors, we hereby declare that:

Our residence, post office address and citizenship are as stated below next to our names;

We believe we are the original, first and joint inventors of the subject matter which is claimed and for which a patent is sought on the invention entitled AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES, the specification of which

- ☒ is attached hereto.
- ☐ was filed on _____as Application Serial Number _____and was amended on _____ (if applicable).
- ☐ was filed under the Patent Cooperation Treaty (PCT) and accorded International Application No. _____, filed _____, and amended on _____ (if any).

We hereby state that we have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

We hereby acknowledge the duty to disclose information which is material to patentability in accordance with Title 37, Code of Federal Regulations, §1.56(a).

Prior Foreign Application(s)

We hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application(s) for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Country	Application No.	Date of Filing (day month year)	Date of Issue (day month year)	Priority Claimed Under 35 U.S.C. §119

Prior United States Provisional Application(s)

We hereby claim priority benefits under Title 35, United States Code, §119(e)(1) of any U.S. provisional application listed below:

U.S. Provisional Application No.	Date of Filing (day month year)	Priority Claimed Under 35 U.S.C. §119(e)(1)
60/106,261	30 October 1998	Yes
60/137,704	7 June 1999	Yes

Prior United States Application(s)

We hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, we acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Petitioner Apple Inc. - Exhibit 1002, p. 149

Application Serial No.	Date of Filing (Day, Month, Year)	Status — Patented, Pending, Abandoned
09/558,210	26 April 2000	Pending
09/504,783	15 February 2000	Patented
09/429,643	29 October 1999	Pending

Power of Attorney

And we hereby appoint, both jointly and severally, as our attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith the practitioners at:

Customer Number: 22907 (WDC)

Please address all correspondence and telephone communications to the address and telephone number for this Customer Number.

We hereby declare that all statements made herein of our own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Signature_____ Date_____
Full Name of First Inventor____ Larson (Family Name) Victor (First Given Name) ____ (Second Given Name)
Residence Fairfax, Virginia Citizenship USA
Post Office Address 12026 Lisa Marie Court, Fairfax, Virginia 22033

Signature_____ Date_____
Full Name of Second Inventor____ Short, III (Family Name) Robert (First Given Name) Dunham (Second Given Name)
Residence Leesburg, Virginia Citizenship USA
Post Office Address 38710 Goose Creek Lane, Leesburg, Virginia 20175

Signature Edmund Colby Munger Date 11 November 2003
Full Name of Third Inventor____ Munger (Family Name) Edmund (First Given Name) Colby (Second Given Name)
Residence Crownsville, Maryland Citizenship USA
Post Office Address 1101 Opaca Court, Crownsville, Maryland 21032

Signature_____ Date_____
Full Name of Fourth Inventor____ Williamson (Family Name) Michael (First Given Name) ____ (Second Given Name)
Residence South Riding, Virginia Citizenship USA
Post Office Address 26203 Ocala Circle, South Riding, Virginia 20152

Petitioner Apple Inc. - Exhibit 1002, p. 150

Doc Code: 077580 - 0063

PTO/SB/80 (01-06)
Approved for use through 12/31/2008. OMB 0651-0035
U S. Patent and Trademark Office; U S DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

I hereby appoint:

☒ Practitioners associated with the Customer — 23,630

OR

☐ Practitioner(s) named below (if more then ten practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to:

☒ The address associated with Customer — 23,630

OR

☒ Firm or Individual Name	McDermott Will & Emery LLP		
Address	28 State Street		
City	Boston	State MA	Zip 02109
Country	U.S.A.		
Telephone	(617) 535-4065	Email tkusmer@mwe.com	

Assignee Name and Address:
VIRNETX, INC.
5615 SCOTTS VALLEY DRIVE, SUITE 110
SCOTTS VALLEY, CALIFORNIA 95066

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature	Randall Stevens	Date	10/19/07
Name	Randall Carson	Telephone	831.608.5698
Title	President		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/96 (04-07)
Approved for use through 09/30/2007. OMB 0651-0031
U S Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: **VIRNETX, INC.**

Application No./Patent No.: **11/840,560** Filed/Issue Date: **AUGUST 17, 2007**

Entitled: **AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES**

VIRNETX, INC , a **CORPORATION**

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that it is:

1. ☑ the assignee of the entire right, title, and interest; or

2. ☐ an assignee of less than the entire right, title and interest
(The extent (by percentage) of its ownership interest is _____ %)

in the patent application/patent identified above by virtue of either:

A. ☐ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attatched.

OR

B. ☑ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: Victor Larson, et al. To: Science Applications International Corporation
The document was recorded in the United States Patent and Trademark Office at
Reel 019722, Frame 0321, or for which a copy thereof is attached.

2. From: Science Applications International Corporation To: VirnetX, Inc
The document was recorded in the United States Patent and Trademark Office at
Reel 019722, Frame 0525, or for which a copy thereof is attached.

3. From: N/A To: _____
The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet.

☐ As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (*i.e.*, a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

Signature — Date: 10/12/07

Printed or Typed Name: Kendall Larson — Telephone number: 831.608.5698

Title: President

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Toby H. Kusmer./Jessica Brown
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)

Filed as Large Entity

Track I Prioritized Examination - Nonprovisional Application under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility application filing	1011	1	380	380
Utility Search Fee	1111	1	620	620
Utility Examination Fee	1311	1	250	250
Request for Prioritized Examination	1817	1	4800	4800
Pages:				
Utility Appl Size fee per 50 sheets >100	1081	1	310	310
Claims:				
Claims in excess of 20	1202	8	60	480

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous-Filing:				
Publ. Fee- early, voluntary, or normal	1504	1	300	300
Processing Fee, except for Provis. apps	1808	1	130	130
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**7270**

Electronic Acknowledgement Receipt

EFS ID:	11703565
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Jessica Brown
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	23-DEC-2011
Filing Date:	
Time Stamp:	16:41:42
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$7270
RAM confirmation Number	3068
Deposit Account	501133
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal of New Application	151Transmittal.pdf	93565 3c8fb9db48d0fbf72fafa27ec5eb688c5c5c9a7c	no	3
Warnings:					
Information:					
2	TrackOne Request	151PrioritizedExamApp.pdf	134470 68e0ff56eae0dc99665a83cc46d4a00edbb04cf3	no	2
Warnings:					
Information:					
3		151Specification.pdf	415145 fc58a3e43fc544744af1c0ce80bd9d7ad8a40fe1	yes	93

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	88
Claims	89	92
Abstract	93	93

Warnings:					
Information:					
4	Drawings-only black and white line drawings	151Figures.pdf	11897155 7580b92bc45fe5d1e5ed25c4b872f77086bebfb1	no	40
Warnings:					
Information:					
5	Application Data Sheet	151ADS.pdf	1032709 5344188bb519250fdedab32d7cf547c5c397c797	no	6
Warnings:					
Information:					
6	Oath or Declaration filed	151Declaration2.pdf	333920 aa7ccb81a15c452ab2f6aed1b0e8c2962332ec98	no	6
Warnings:					
Information:					
7	Power of Attorney	151POA2.pdf	234752 e65ad607d0f9e313687ffe639634c86b302a4395	no	2

Warnings:					
Information:					
8	Fee Worksheet (SB06)	fee-info.pdf	43641 1fb8e1c084cde68026b24a37b9f82b40c96b75b3	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	14185357	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronic Acknowledgement Receipt

EFS ID:	11703565
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Jessica Brown
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	23-DEC-2011
Filing Date:	
Time Stamp:	16:41:42
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$7270
RAM confirmation Number	3068
Deposit Account	501133
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal of New Application	151Transmittal.pdf	93565 3c8fb9db48d0fbf72fafa27ec5eb688c5c5c9a7c	no	3
Warnings:					
Information:					
2	TrackOne Request	151PrioritizedExamApp.pdf	134470 68e0ff56eae0dc99665a83cc46d4a00edbb04cf3	no	2
Warnings:					
Information:					
3		151Specification.pdf	415145 fc58a3e43fc544744af1c0ce80bd9d7ad8a40fe1	yes	93

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	88
Claims	89	92
Abstract	93	93

Warnings:					
Information:					
4	Drawings-only black and white line drawings	151Figures.pdf	11897155 7580b92bc45fe5d1e5ed25c4b872f77086bebfb1	no	40
Warnings:					
Information:					
5	Application Data Sheet	151ADS.pdf	1032709 5344188bb519250fdedab32d7cf547c5c397c797	no	6
Warnings:					
Information:					
6	Oath or Declaration filed	151Declaration2.pdf	333920 aa7ccb81a15c452ab2f6aed1b0e8c2962332ec98	no	6
Warnings:					
Information:					
7	Power of Attorney	151POA2.pdf	234752 e65ad607d0f9e313687ffe639634c86b302a4395	no	2

Warnings:					
Information:					
8	Fee Worksheet (SB06)	fee-info.pdf	43641 1fb8e1c084cde68026b24a37b9f82b40c96b75b3	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	14185357	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Docket No.: 77580-151(VRNK-1CP3CNFT1) **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Customer Number: 23630
LARSON, Victor, et al.	:	Confirmation Number: 6217
Application No.: 13/336,790	:	Group Art Unit: Unknown
Filed: December 23, 2011	:	Examiner: Unknown

For: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this correspondence is being electronically-transmitted to the United States Patent and Trademark Office on **December 23, 2011**

/Jessica Brown/
Jessica Brown

TRANSMITTAL OF REPLACEMENT DRAWINGS FOR TRACK I PRIORITIZED EXAMINATION APPLICATION FILED DECEMBER 23, 2011

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Forty (40) sheets of drawings, Figures 1-37, were filed on this date, December 23, 2011. Forty (40) replacement sheets are being filed herewith, on the same date as the initial filing, showing the page numbering on each sheet, should this be needed.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

/Toby H. Kusmer/
Toby H. Kusmer, P.C., Registration No. 26.418

600 13th Street, N.W.
Washington, D.C. 20005
Phone: (617) 535-4000
Facsimile: (617) 535-3800
Date: December 23, 2011

Please recognize our Customer No. 23630 as our correspondence address.

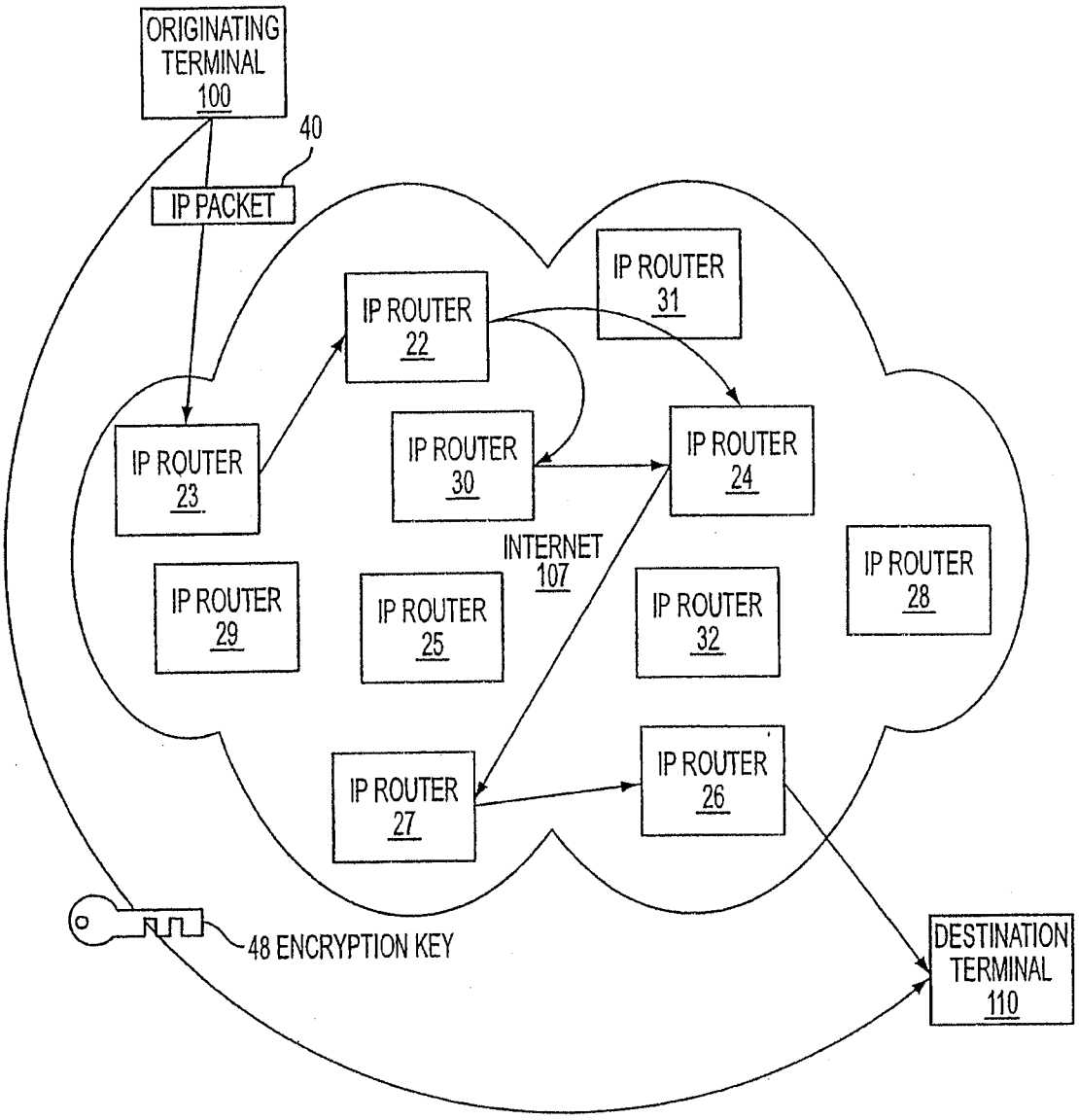

ORIGINATING TERMINAL 100
40
IP PACKET
IP ROUTER 22
IP ROUTER 31
IP ROUTER 23
IP ROUTER 30
IP ROUTER 24
INTERNET 107
IP ROUTER 29
IP ROUTER 25
IP ROUTER 32
IP ROUTER 28
IP ROUTER 27
IP ROUTER 26
48 ENCRYPTION KEY
DESTINATION TERMINAL 110

FIG. 1

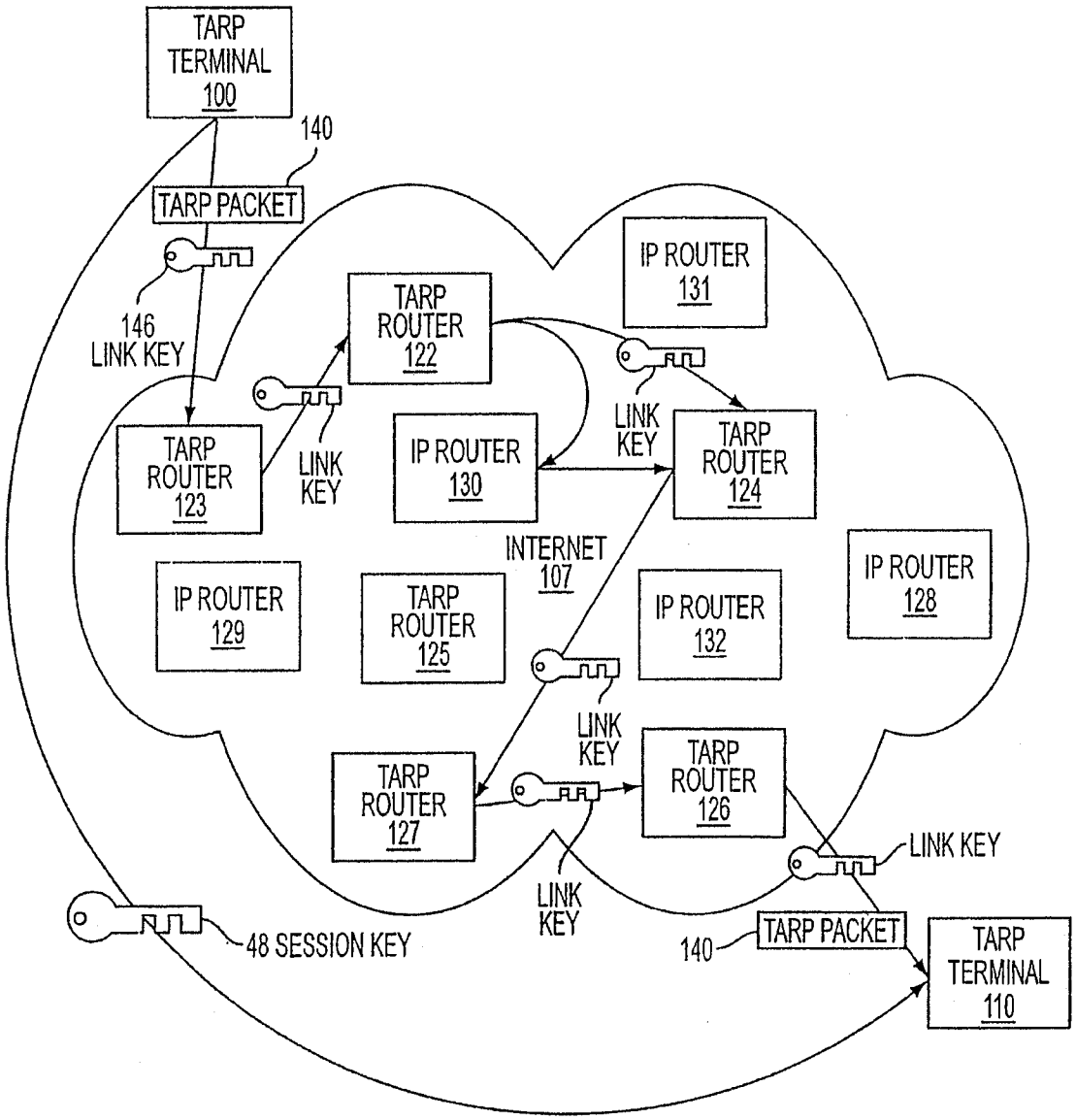

TARP TERMINAL 100
140
TARP PACKET
146 LINK KEY
TARP ROUTER 122
IP ROUTER 131
LINK KEY
TARP ROUTER 123
LINK KEY
IP ROUTER 130
LINK KEY
TARP ROUTER 124
INTERNET 107
IP ROUTER 129
TARP ROUTER 125
IP ROUTER 132
IP ROUTER 128
LINK KEY
TARP ROUTER 127
TARP ROUTER 126
LINK KEY
LINK KEY
48 SESSION KEY
140
TARP PACKET
TARP TERMINAL 110

FIG. 2

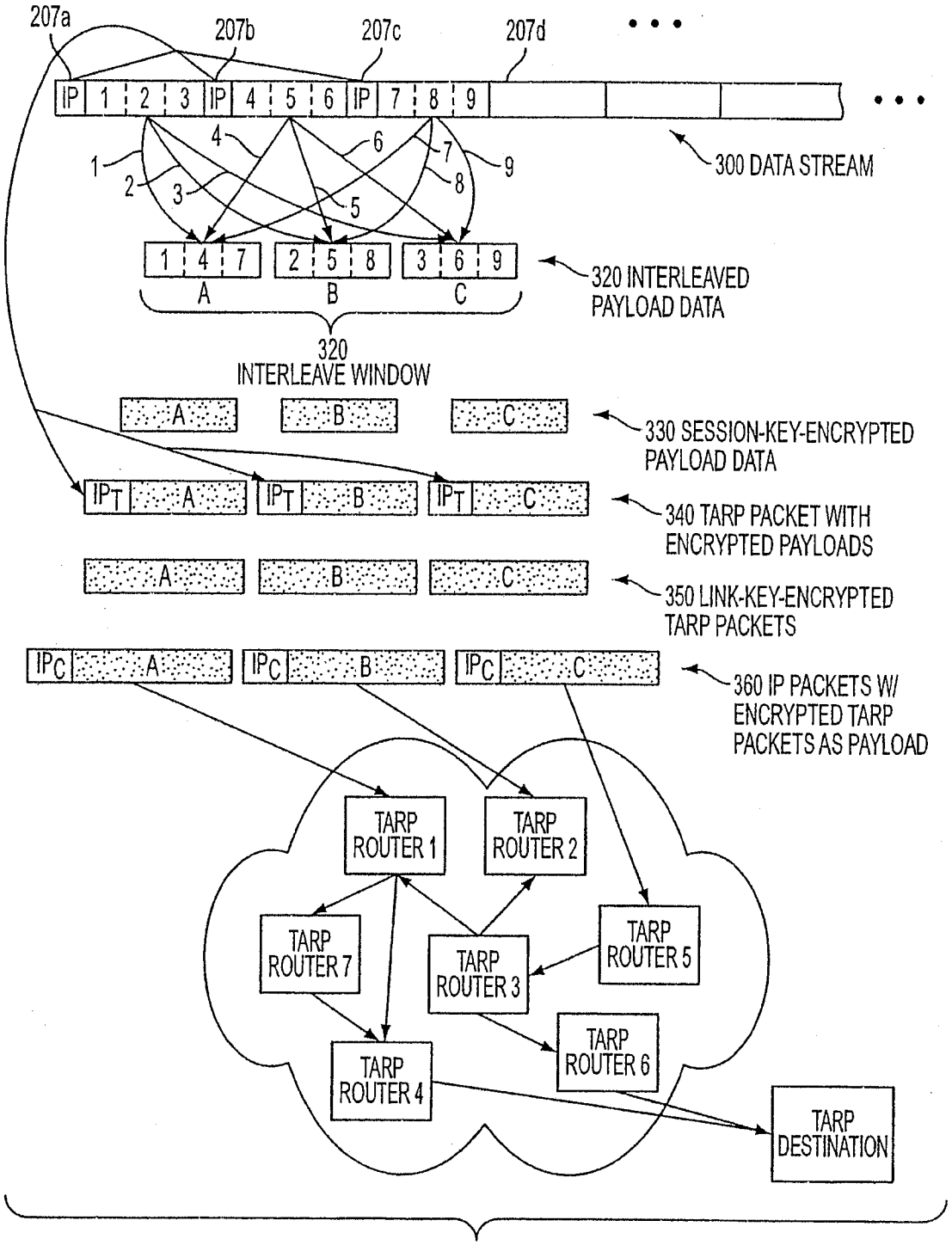

207a
207b
207c
207d
IP 1 2 3 IP 4 5 6 IP 7 8 9
300 DATA STREAM
1 4 7
2 5 8
3 6 9
A
B
C
320 INTERLEAVED PAYLOAD DATA
320 INTERLEAVE WINDOW
330 SESSION-KEY-ENCRYPTED PAYLOAD DATA
IPT A IPT B IPT C
340 TARP PACKET WITH ENCRYPTED PAYLOADS
350 LINK-KEY-ENCRYPTED TARP PACKETS
IPC A IPC B IPC C
360 IP PACKETS W/ ENCRYPTED TARP PACKETS AS PAYLOAD
TARP ROUTER 1
TARP ROUTER 2
TARP ROUTER 7
TARP ROUTER 3
TARP ROUTER 5
TARP ROUTER 4
TARP ROUTER 6
TARP DESTINATION

FIG. 3A

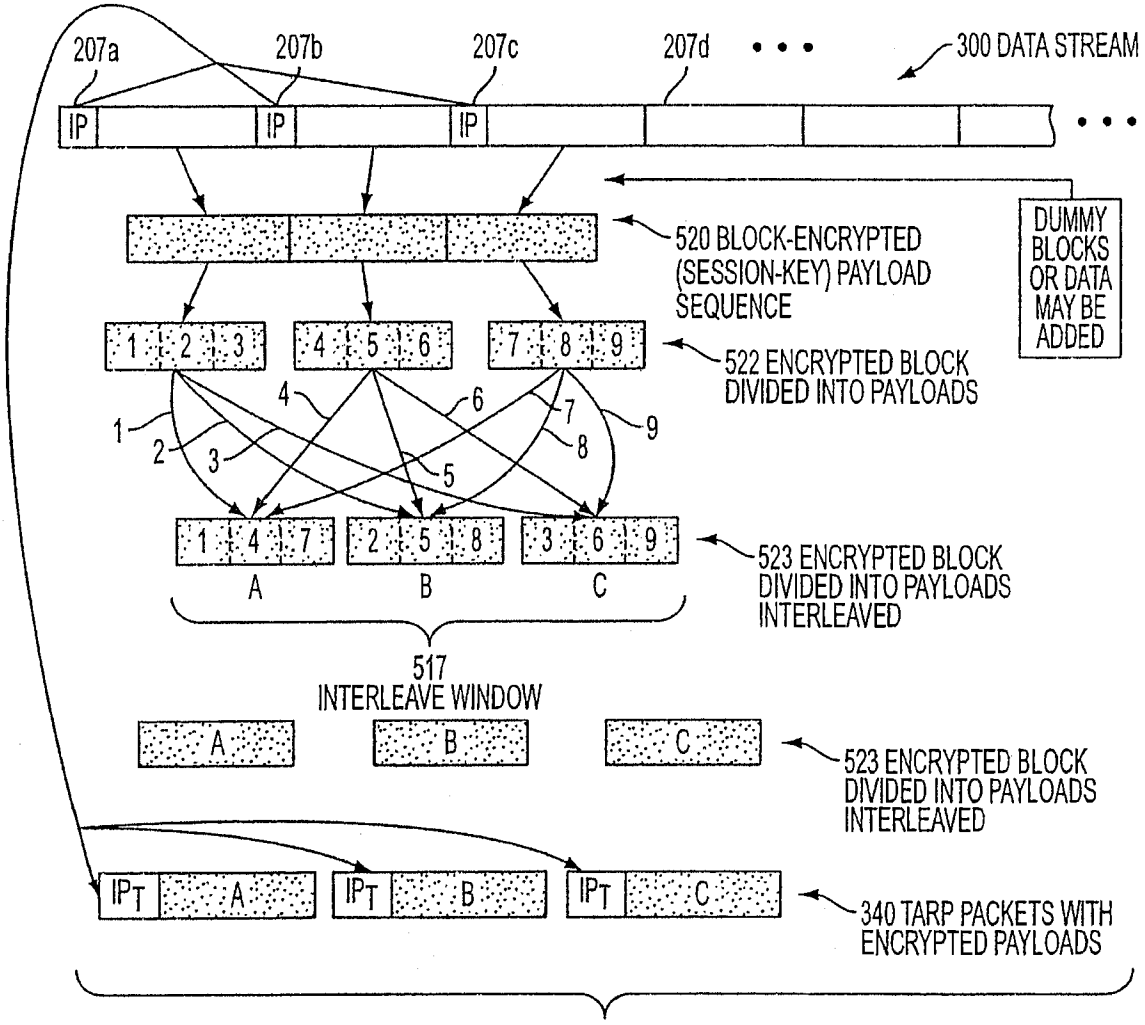

207a
207b
207c
207d
300 DATA STREAM
IP
IP
IP
520 BLOCK-ENCRYPTED (SESSION-KEY) PAYLOAD SEQUENCE
DUMMY BLOCKS OR DATA MAY BE ADDED
1 2 3
4 5 6
7 8 9
522 ENCRYPTED BLOCK DIVIDED INTO PAYLOADS
1 4 7
2 5 8
3 6 9
A
B
C
523 ENCRYPTED BLOCK DIVIDED INTO PAYLOADS INTERLEAVED
517
INTERLEAVE WINDOW
A
B
C
523 ENCRYPTED BLOCK DIVIDED INTO PAYLOADS INTERLEAVED
IPT A
IPT B
IPT C
340 TARP PACKETS WITH ENCRYPTED PAYLOADS

FIG. 3B

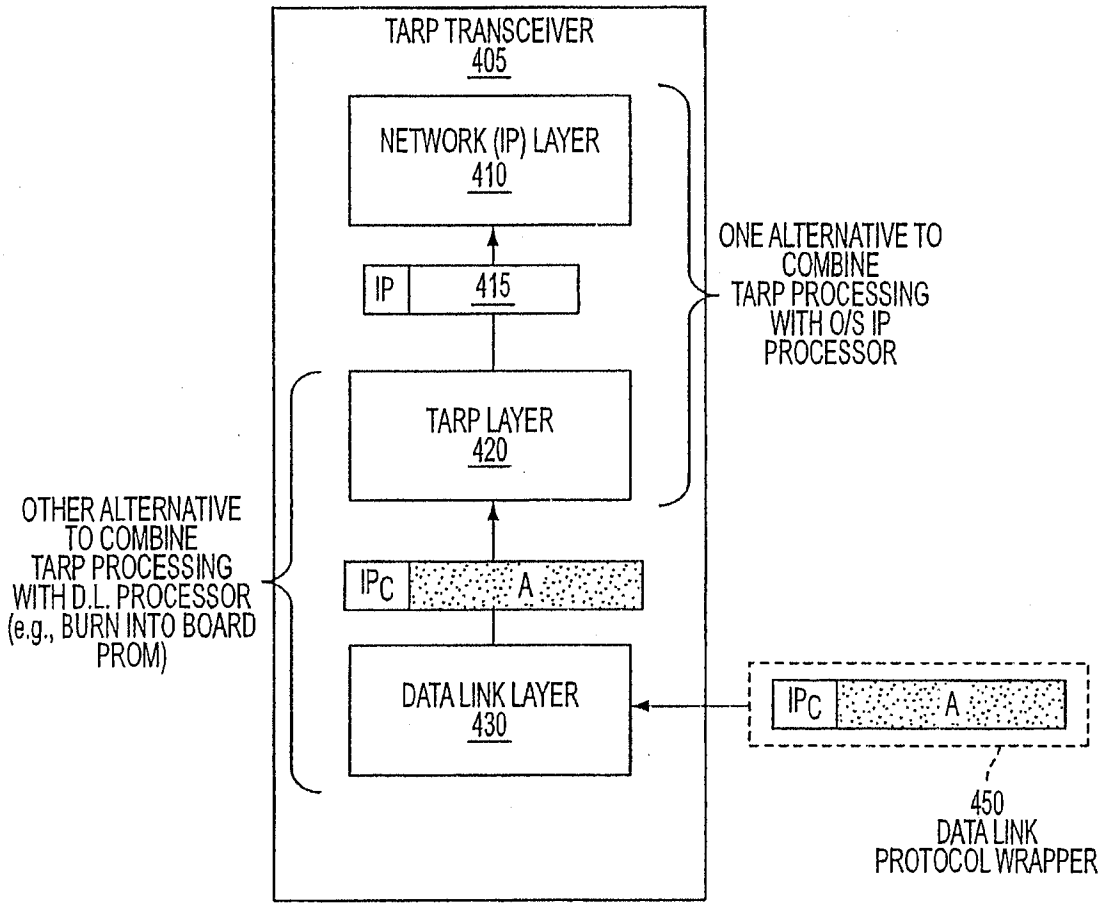

TARP TRANSCEIVER
405
NETWORK (IP) LAYER
410
IP
415
TARP LAYER
420
IPC
A
DATA LINK LAYER
430
ONE ALTERNATIVE TO COMBINE TARP PROCESSING WITH O/S IP PROCESSOR
OTHER ALTERNATIVE TO COMBINE TARP PROCESSING WITH D.L. PROCESSOR (e.g., BURN INTO BOARD PROM)
IPC
A
450
DATA LINK PROTOCOL WRAPPER

FIG. 4

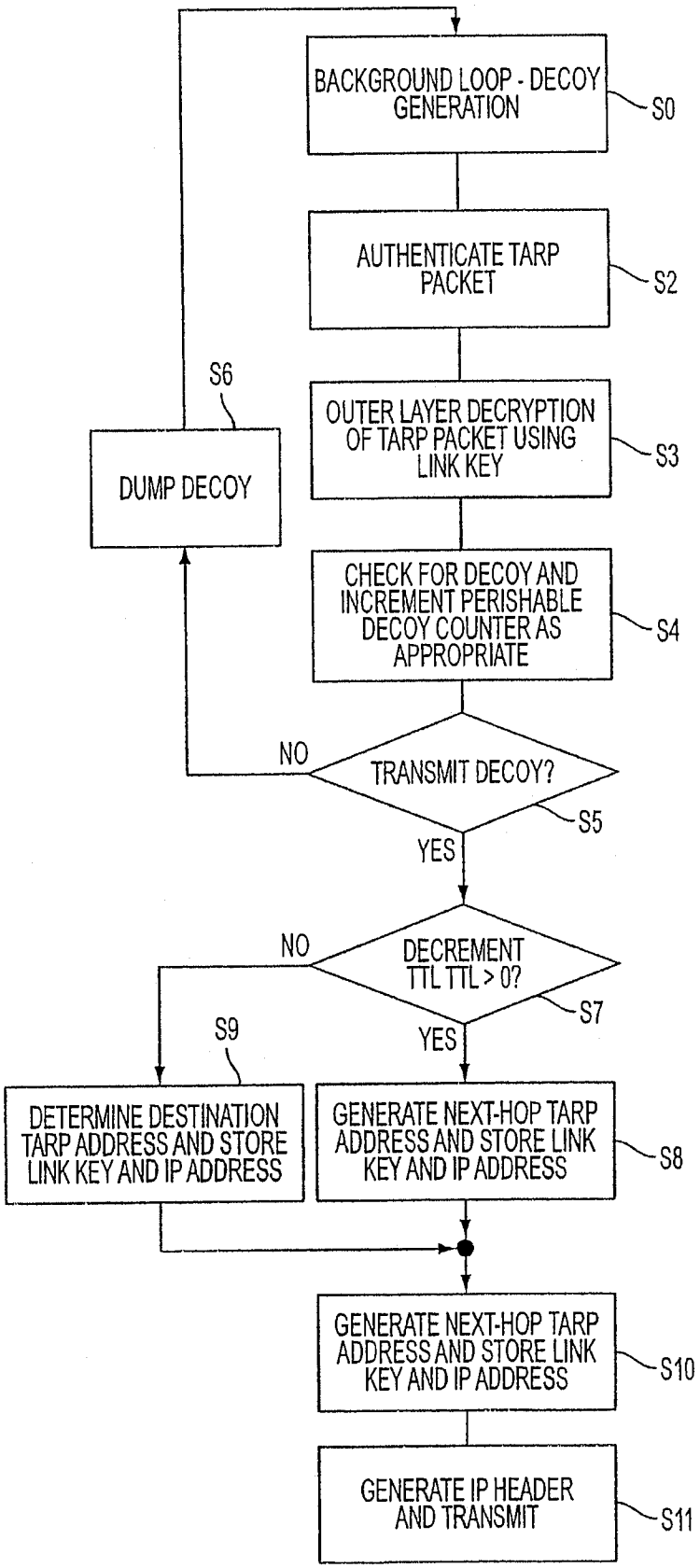

BACKGROUND LOOP - DECOY GENERATION
S0
AUTHENTICATE TARP PACKET
S2
OUTER LAYER DECRYPTION OF TARP PACKET USING LINK KEY
S3
CHECK FOR DECOY AND INCREMENT PERISHABLE DECOY COUNTER AS APPROPRIATE
S4
TRANSMIT DECOY?
S5
NO
YES
S6
DUMP DECOY
DECREMENT TTL TTL > 0?
S7
NO
YES
S9
DETERMINE DESTINATION TARP ADDRESS AND STORE LINK KEY AND IP ADDRESS
GENERATE NEXT-HOP TARP ADDRESS AND STORE LINK KEY AND IP ADDRESS
S8
GENERATE NEXT-HOP TARP ADDRESS AND STORE LINK KEY AND IP ADDRESS
S10
GENERATE IP HEADER AND TRANSMIT
S11

FIG. 5

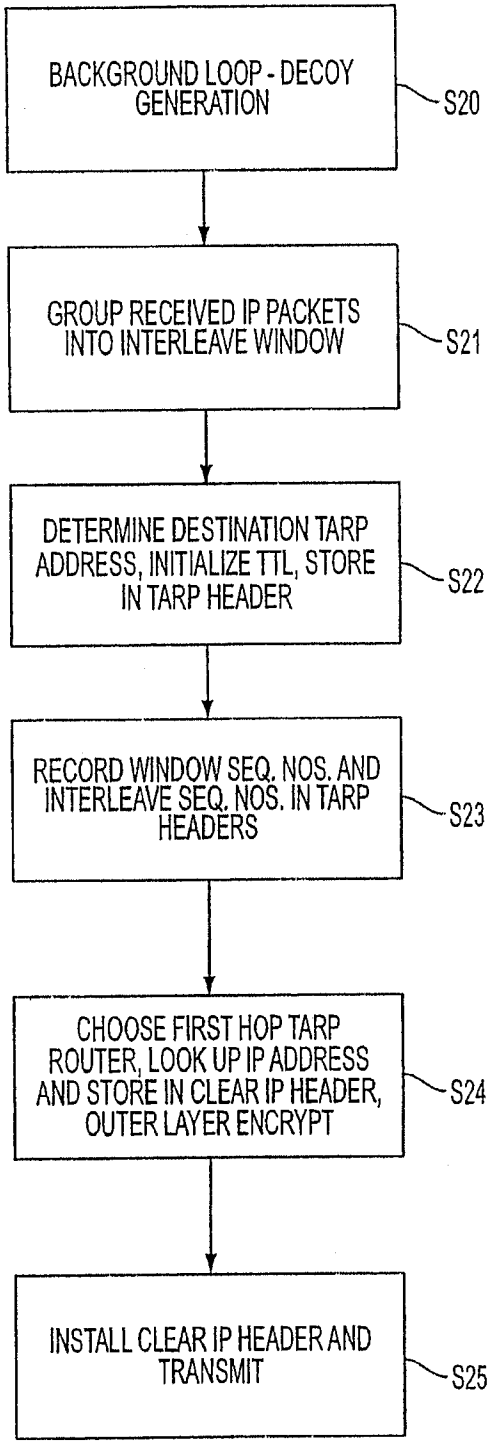

BACKGROUND LOOP - DECOY GENERATION
S20
GROUP RECEIVED IP PACKETS INTO INTERLEAVE WINDOW
S21
DETERMINE DESTINATION TARP ADDRESS, INITIALIZE TTL, STORE IN TARP HEADER
S22
RECORD WINDOW SEQ. NOS. AND INTERLEAVE SEQ. NOS. IN TARP HEADERS
S23
CHOOSE FIRST HOP TARP ROUTER, LOOK UP IP ADDRESS AND STORE IN CLEAR IP HEADER, OUTER LAYER ENCRYPT
S24
INSTALL CLEAR IP HEADER AND TRANSMIT
S25

FIG. 6

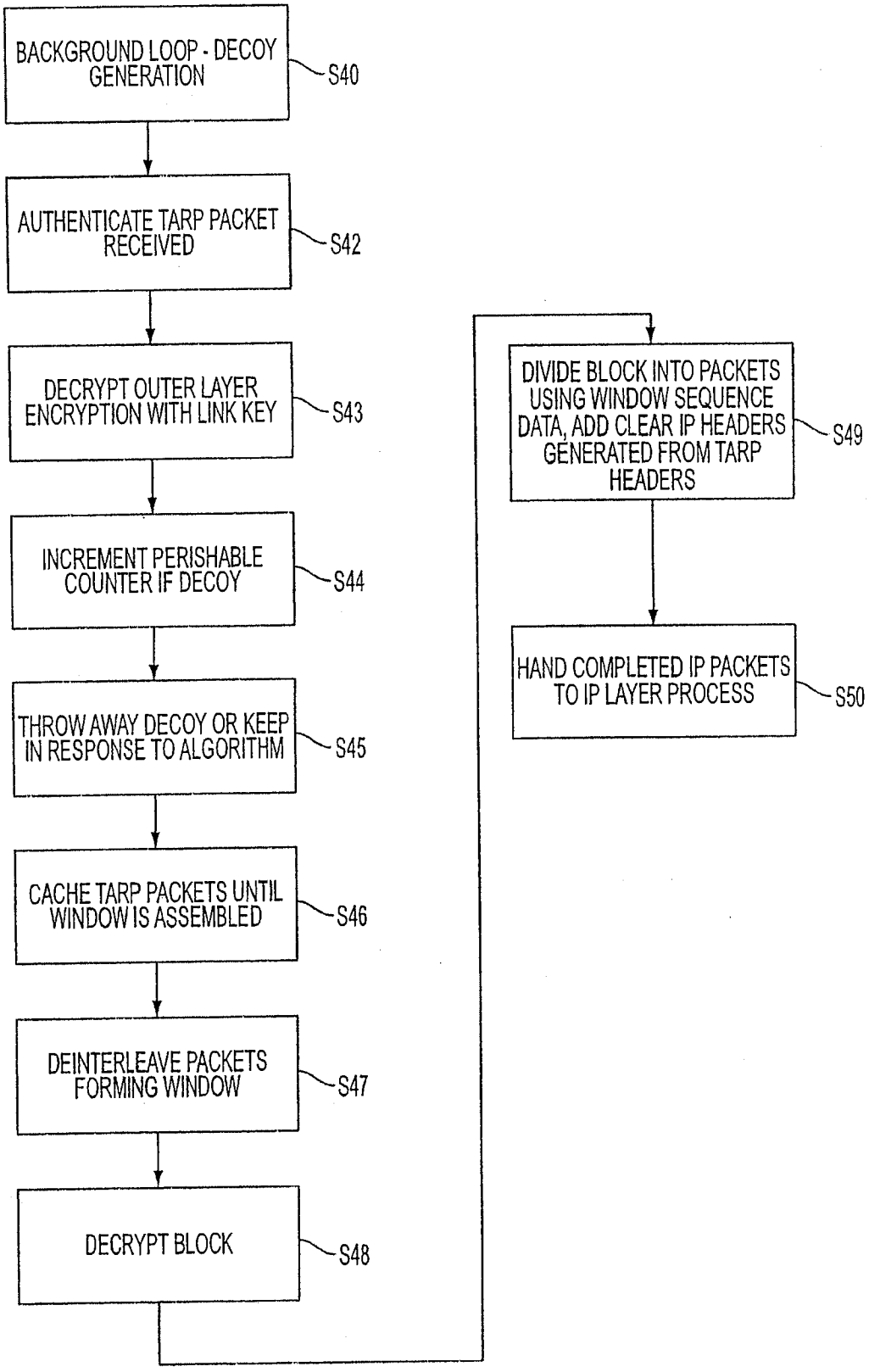

BACKGROUND LOOP - DECOY GENERATION
S40
AUTHENTICATE TARP PACKET RECEIVED
S42
DECRYPT OUTER LAYER ENCRYPTION WITH LINK KEY
S43
INCREMENT PERISHABLE COUNTER IF DECOY
S44
THROW AWAY DECOY OR KEEP IN RESPONSE TO ALGORITHM
S45
CACHE TARP PACKETS UNTIL WINDOW IS ASSEMBLED
S46
DEINTERLEAVE PACKETS FORMING WINDOW
S47
DECRYPT BLOCK
S48
DIVIDE BLOCK INTO PACKETS USING WINDOW SEQUENCE DATA, ADD CLEAR IP HEADERS GENERATED FROM TARP HEADERS
S49
HAND COMPLETED IP PACKETS TO IP LAYER PROCESS
S50

FIG. 7

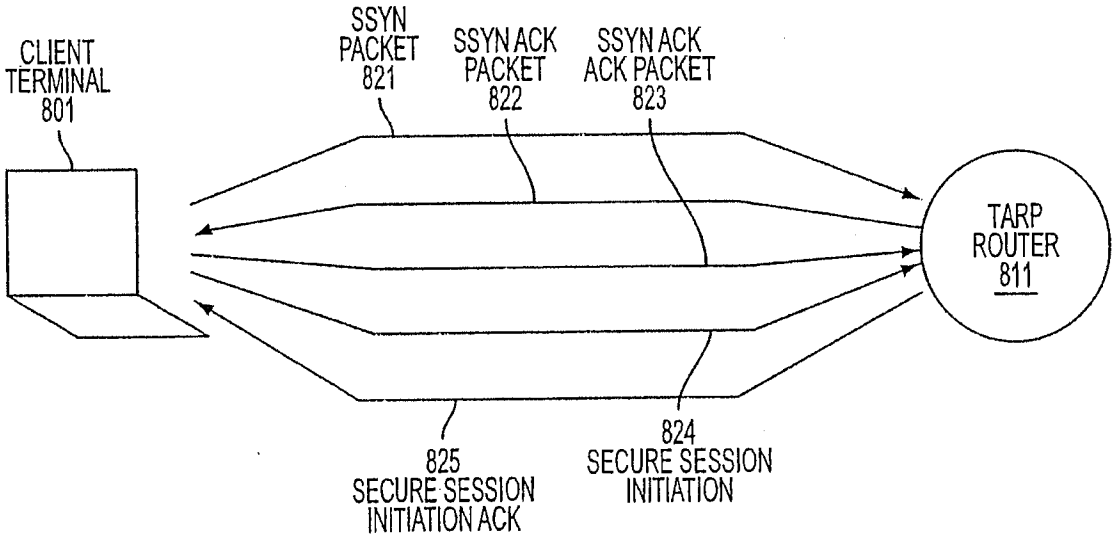

CLIENT TERMINAL 801
SSYN PACKET 821
SSYN ACK PACKET 822
SSYN ACK ACK PACKET 823
TARP ROUTER 811
825 SECURE SESSION INITIATION ACK
824 SECURE SESSION INITIATION

FIG. 8

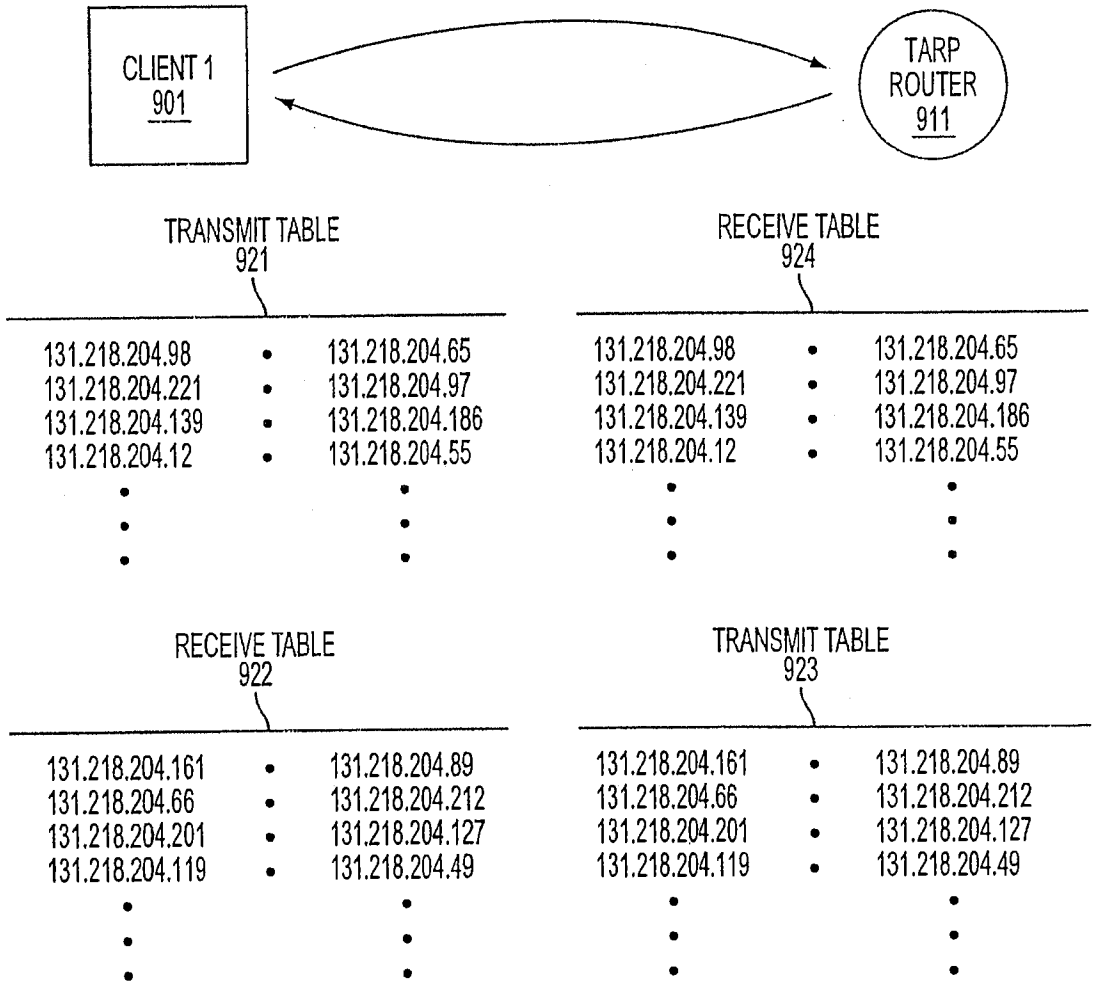

CLIENT 1
901
TARP
ROUTER
911
TRANSMIT TABLE
921
131.218.204.98 • 131.218.204.65
131.218.204.221 • 131.218.204.97
131.218.204.139 • 131.218.204.186
131.218.204.12 • 131.218.204.55
RECEIVE TABLE
924
131.218.204.98 • 131.218.204.65
131.218.204.221 • 131.218.204.97
131.218.204.139 • 131.218.204.186
131.218.204.12 • 131.218.204.55
RECEIVE TABLE
922
131.218.204.161 • 131.218.204.89
131.218.204.66 • 131.218.204.212
131.218.204.201 • 131.218.204.127
131.218.204.119 • 131.218.204.49
TRANSMIT TABLE
923
131.218.204.161 • 131.218.204.89
131.218.204.66 • 131.218.204.212
131.218.204.201 • 131.218.204.127
131.218.204.119 • 131.218.204.49

FIG. 9

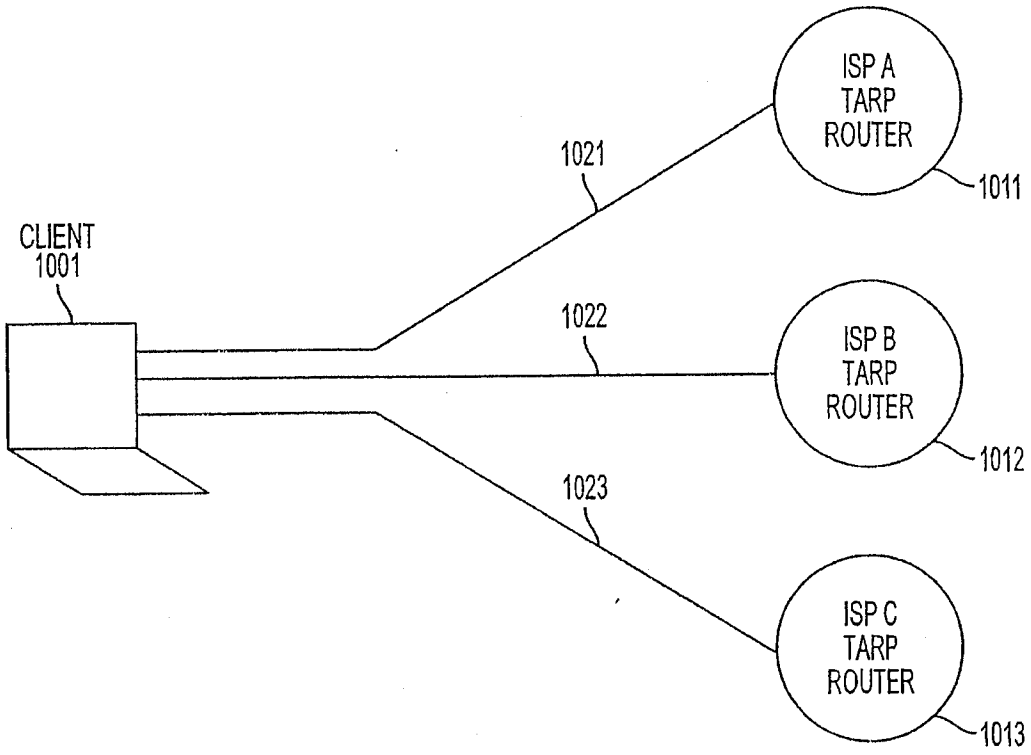

ISP A
TARP
ROUTER
1011
1021
CLIENT
1001
1022
ISP B
TARP
ROUTER
1012
1023
ISP C
TARP
ROUTER
1013

FIG. 10

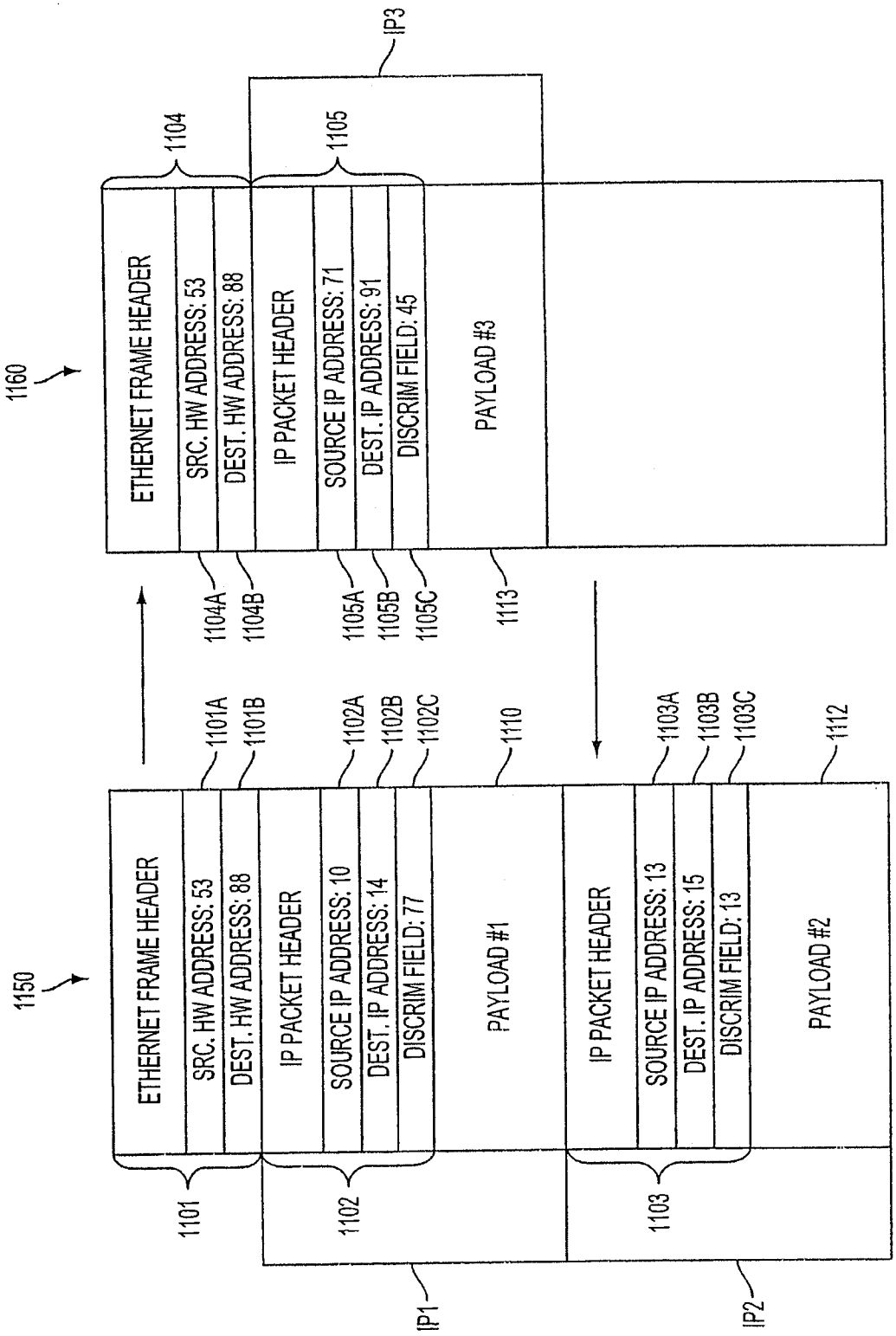

1160
1150
ETHERNET FRAME HEADER
SRC. HW ADDRESS: 53
DEST. HW ADDRESS: 88
IP PACKET HEADER
SOURCE IP ADDRESS: 10
DEST. IP ADDRESS: 14
DISCRIM FIELD: 77
PAYLOAD #1
IP PACKET HEADER
SOURCE IP ADDRESS: 13
DEST. IP ADDRESS: 15
DISCRIM FIELD: 13
PAYLOAD #2
ETHERNET FRAME HEADER
SRC. HW ADDRESS: 53
DEST. HW ADDRESS: 88
IP PACKET HEADER
SOURCE IP ADDRESS: 71
DEST. IP ADDRESS: 91
DISCRIM FIELD: 45
PAYLOAD #3
1101
1102
1103
1104
1105
IP1
IP2
IP3
1101A
1101B
1102A
1102B
1102C
1103A
1103B
1103C
1104A
1104B
1105A
1105B
1105C
1110
1112
1113

FIG. 11

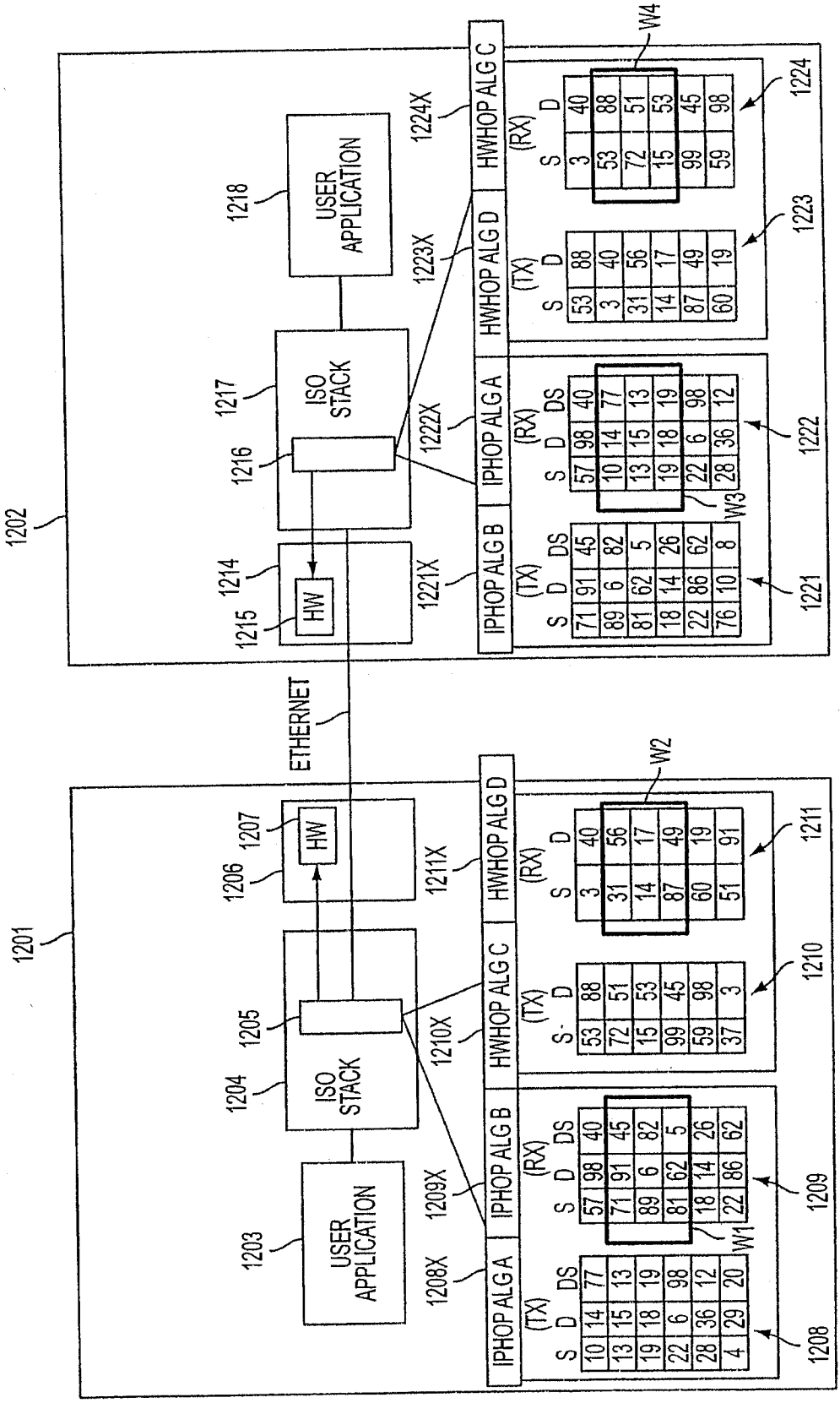

1201
1202
ETHERNET
1203
USER APPLICATION
1204
ISO STACK
1205
1206
1207
HW
1208
1208X
IPHOP ALG A
1209
1209X
IPHOP ALG B
1210
1210X
HWHOP ALG C
1211
1211X
HWHOP ALG D
1214
1215
HW
1216
1217
ISO STACK
1218
USER APPLICATION
1221
1221X
IPHOP ALG B
1222
1222X
IPHOP ALG A
1223
1223X
HWHOP ALG D
1224
1224X
HWHOP ALG C
W1
W2
W3
W4
(TX)
(RX)
S
D
DS

FIG. 12A

MODE OR EMBODIMENT	HARDWARE ADDRESSES	IP ADDRESSES	DISCRIMINATOR FIELD VALUES
1. PROMISCUOUS	SAME FOR ALL NODES OR COMPLETELY RANDOM	CAN BE VARIED IN SYNC	CAN BE VARIED IN SYNC
2. PROMISCUOUS PER VPN	FIXED FOR EACH VPN	CAN BE VARIED IN SYNC	CAN BE VARIED IN SYNC
3. HARDWARE HOPPING	CAN BE VARIED IN SYNC	CAN BE VARIED IN SYNC	CAN BE VARIED IN SYNC

FIG. 12B

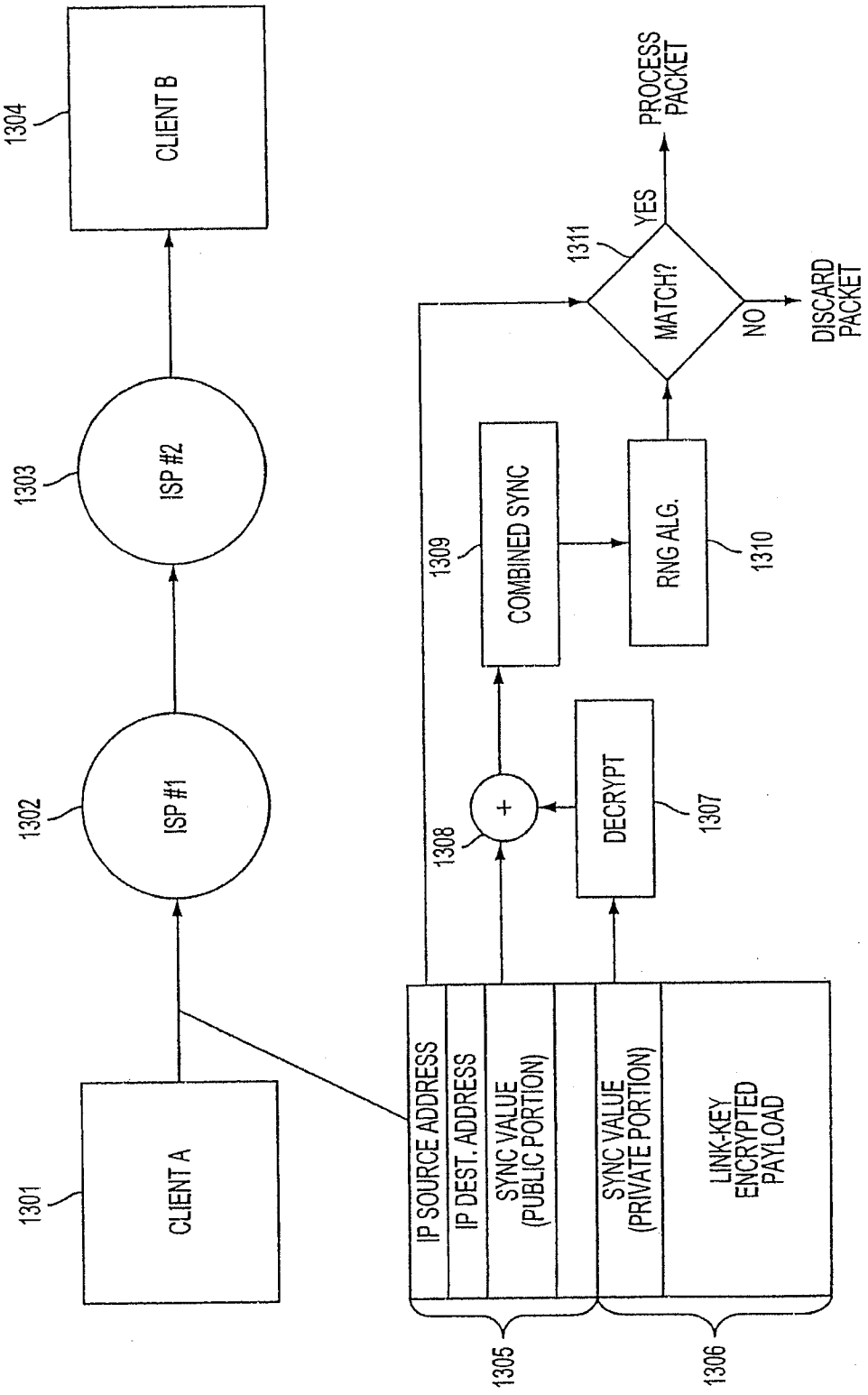

CLIENT A
1301
ISP #1
1302
ISP #2
1303
CLIENT B
1304
IP SOURCE ADDRESS
IP DEST. ADDRESS
SYNC VALUE (PUBLIC PORTION)
SYNC VALUE (PRIVATE PORTION)
LINK-KEY ENCRYPTED PAYLOAD
1305
1306
DECRYPT
1307
+
1308
COMBINED SYNC
1309
RNG ALG.
1310
MATCH?
1311
YES
PROCESS PACKET
NO
DISCARD PACKET

FIG. 13

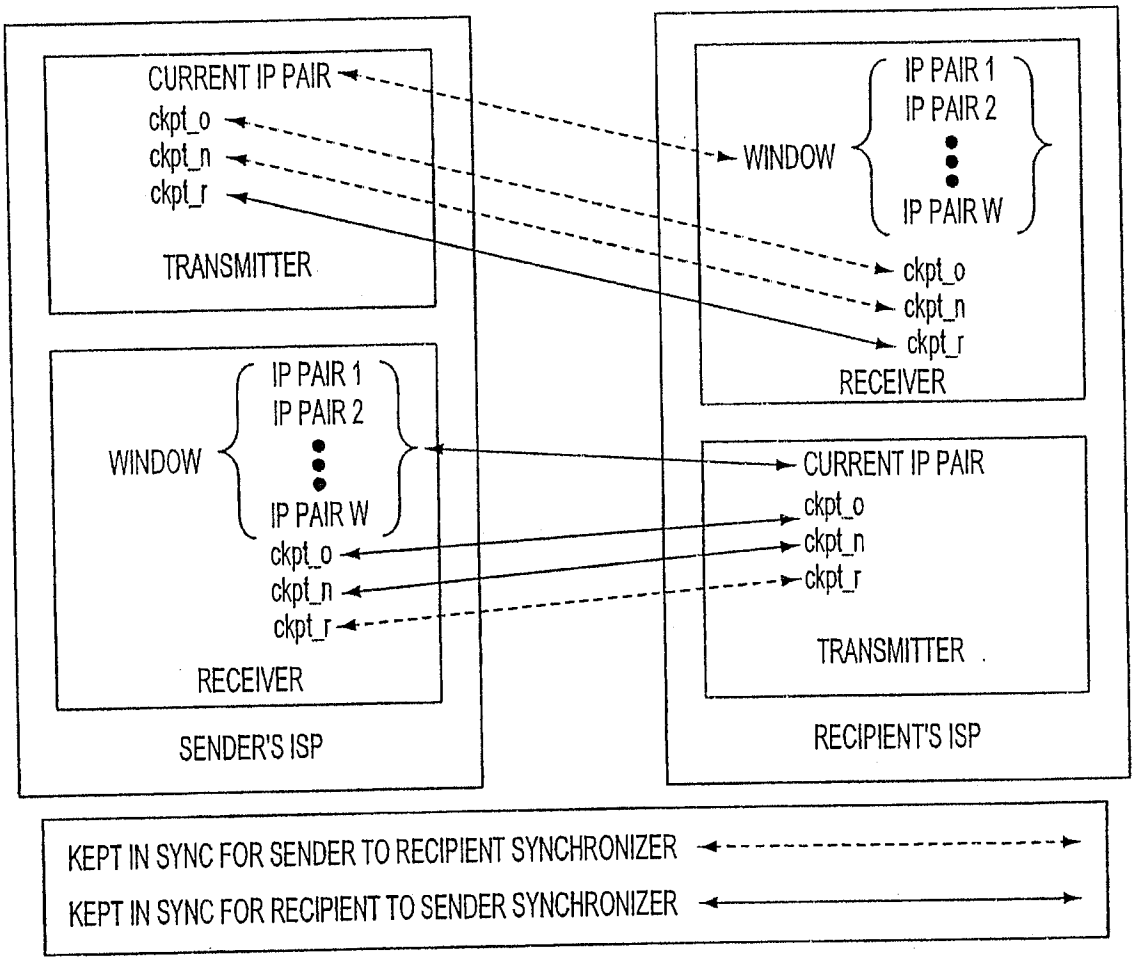

CURRENT IP PAIR
ckpt_o
ckpt_n
ckpt_r
TRANSMITTER
WINDOW
IP PAIR 1
IP PAIR 2
IP PAIR W
ckpt_o
ckpt_n
ckpt_r
RECEIVER
SENDER'S ISP
WINDOW
IP PAIR 1
IP PAIR 2
IP PAIR W
ckpt_o
ckpt_n
ckpt_r
RECEIVER
CURRENT IP PAIR
ckpt_o
ckpt_n
ckpt_r
TRANSMITTER
RECIPIENT'S ISP
KEPT IN SYNC FOR SENDER TO RECIPIENT SYNCHRONIZER
KEPT IN SYNC FOR RECIPIENT TO SENDER SYNCHRONIZER

FIG. 14

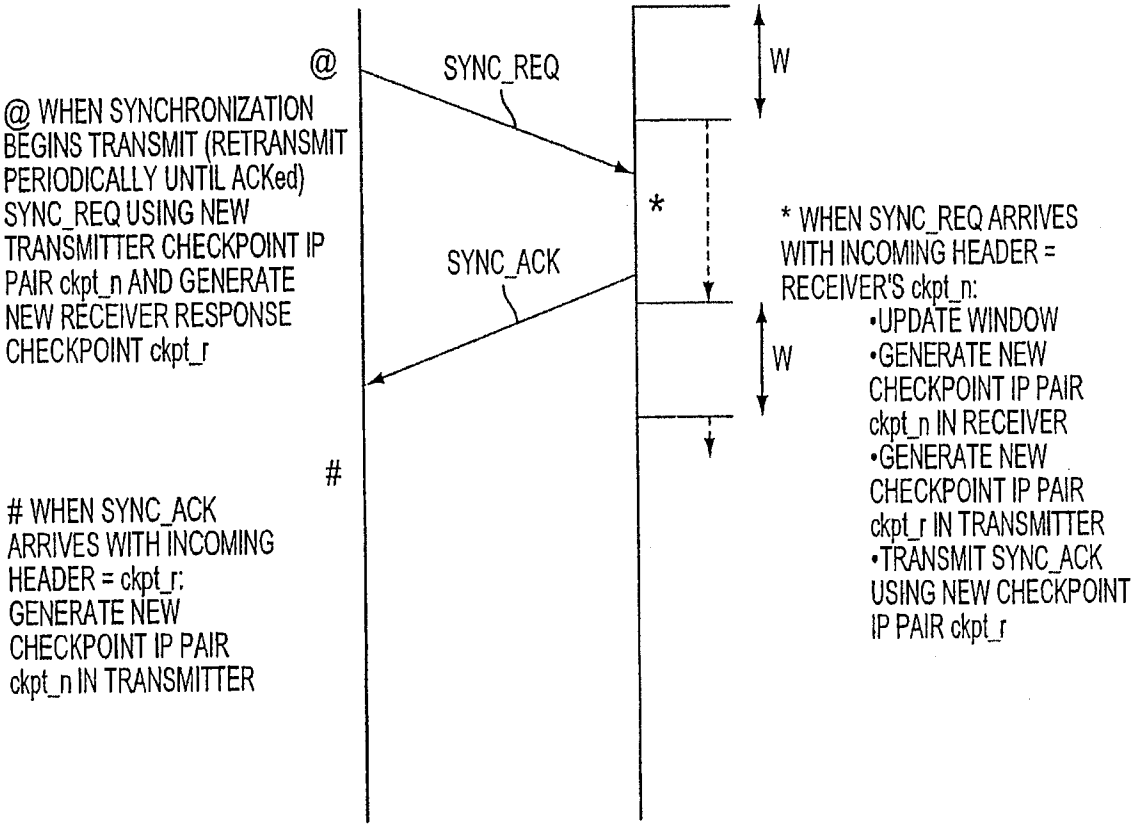

@
SYNC_REQ
W
@ WHEN SYNCHRONIZATION BEGINS TRANSMIT (RETRANSMIT PERIODICALLY UNTIL ACKed) SYNC_REQ USING NEW TRANSMITTER CHECKPOINT IP PAIR ckpt_n AND GENERATE NEW RECEIVER RESPONSE CHECKPOINT ckpt_r
*
* WHEN SYNC_REQ ARRIVES WITH INCOMING HEADER = RECEIVER'S ckpt_n:
•UPDATE WINDOW
•GENERATE NEW CHECKPOINT IP PAIR ckpt_n IN RECEIVER
•GENERATE NEW CHECKPOINT IP PAIR ckpt_r IN TRANSMITTER
•TRANSMIT SYNC_ACK USING NEW CHECKPOINT IP PAIR ckpt_r
SYNC_ACK
W
#
WHEN SYNC_ACK ARRIVES WITH INCOMING HEADER = ckpt_r: GENERATE NEW CHECKPOINT IP PAIR ckpt_n IN TRANSMITTER

FIG. 15

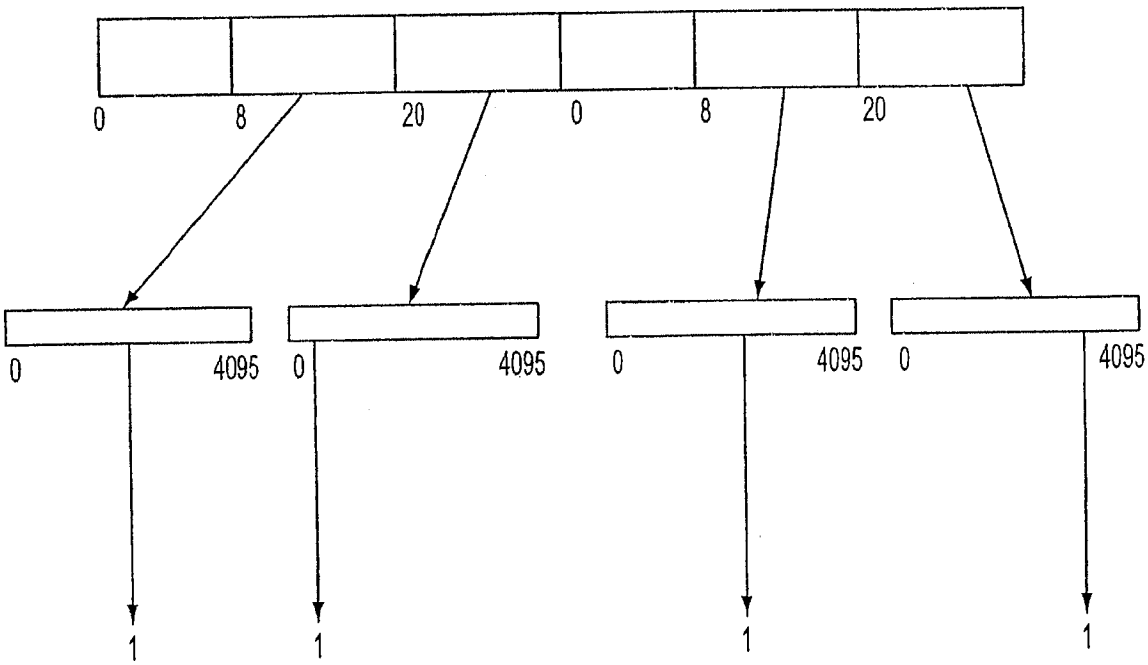


FIG. 16

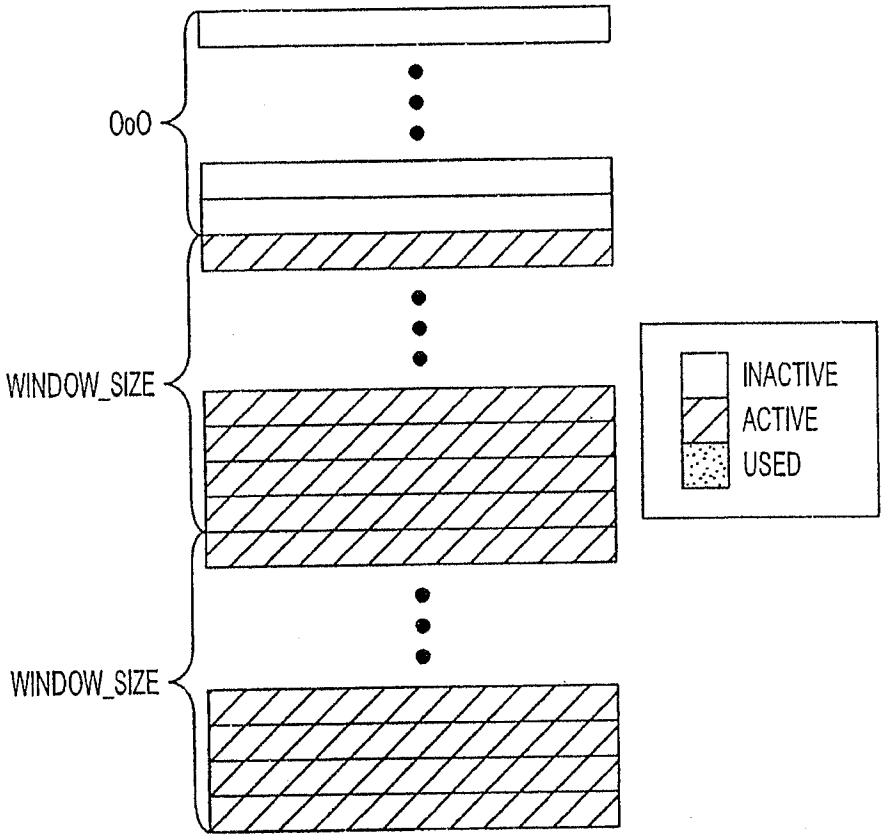


FIG. 17

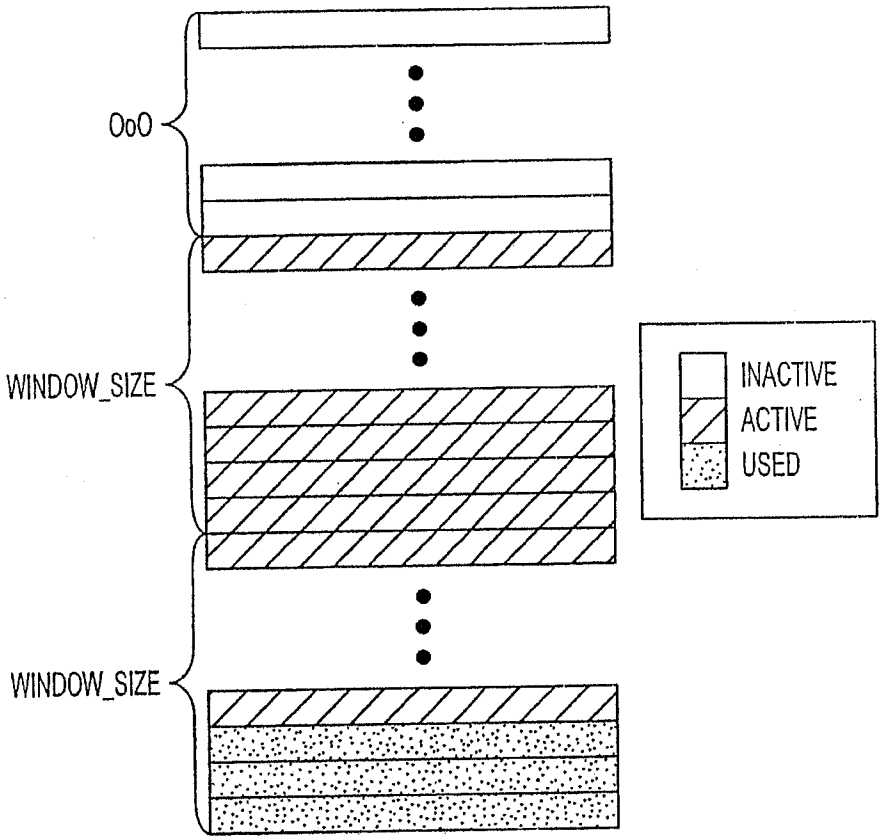


FIG. 18

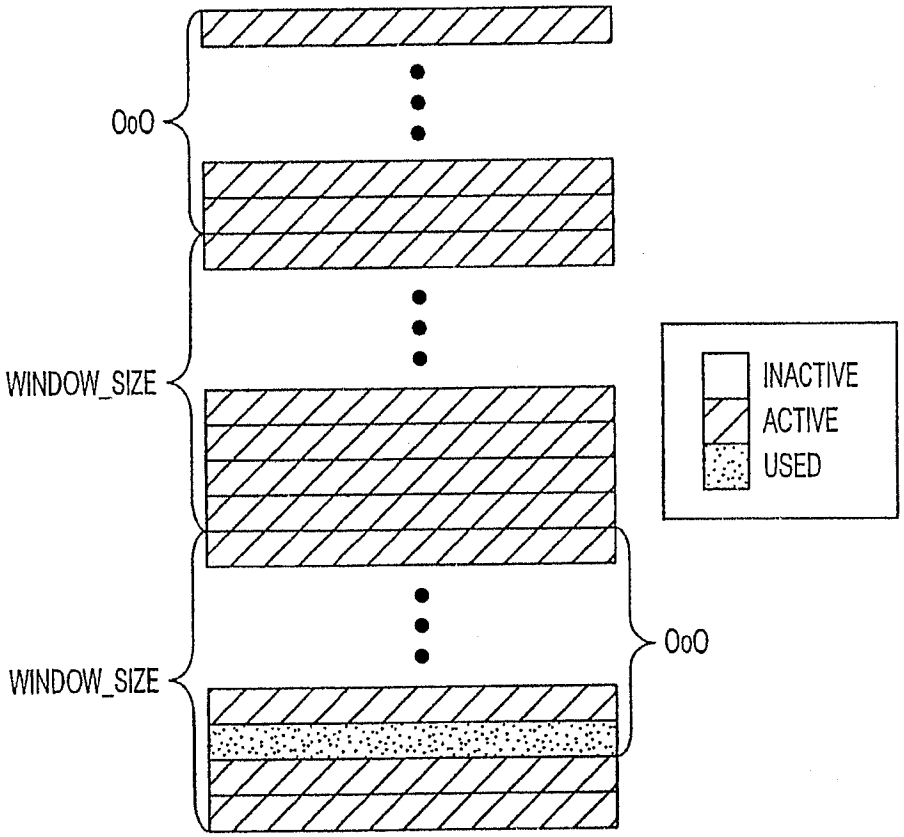


FIG. 19

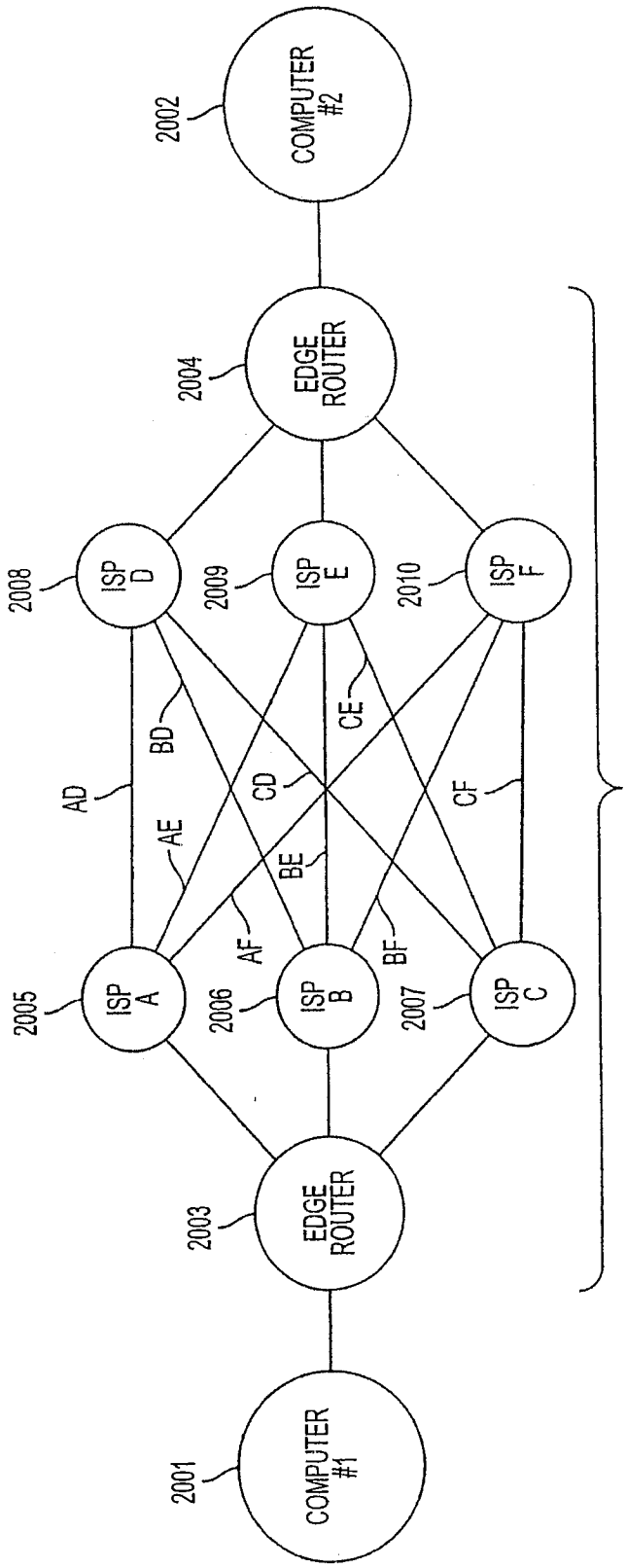

COMPUTER #2
2002
EDGE ROUTER
2004
ISP D
2008
ISP E
2009
ISP F
2010
AD
BD
CD
CE
CF
AE
AF
BE
BF
ISP A
2005
ISP B
2006
ISP C
2007
EDGE ROUTER
2003
COMPUTER #1
2001
2011

FIG. 20

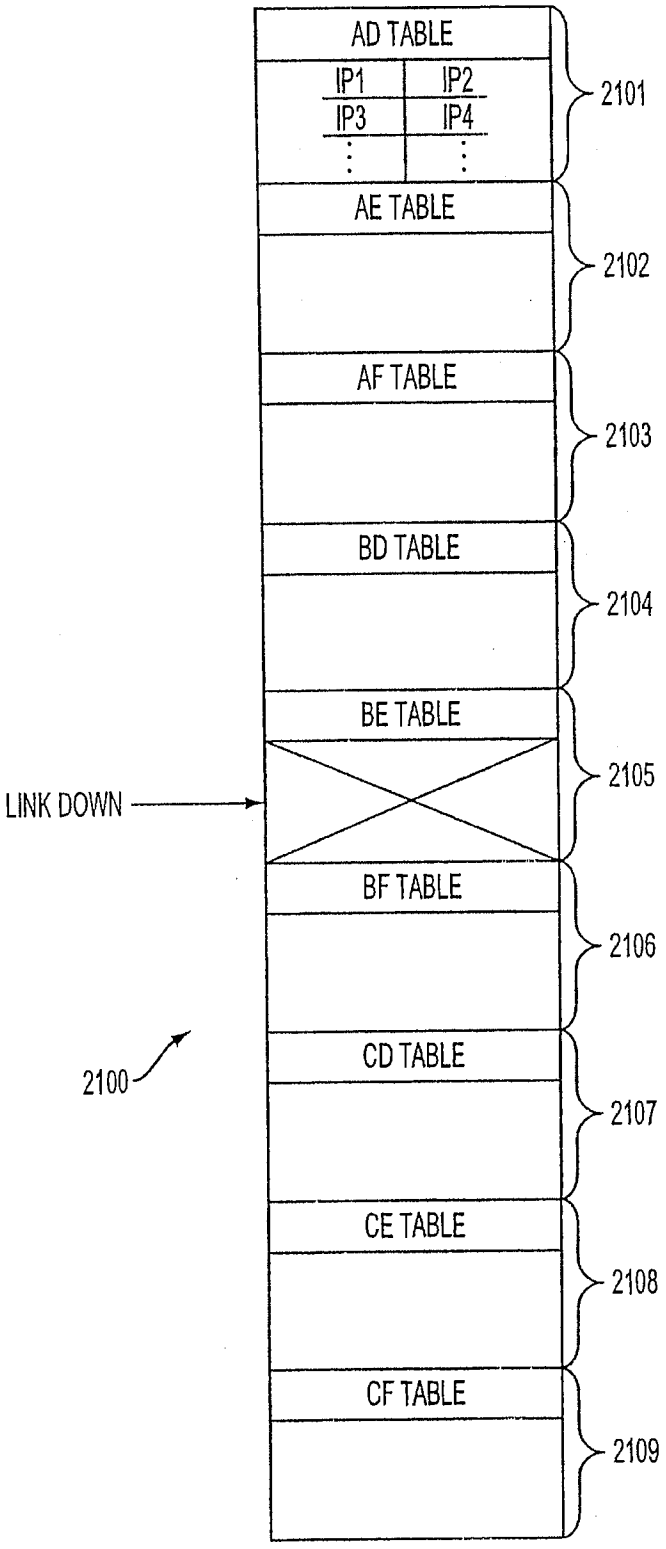

AD TABLE
IP1
IP2
IP3
IP4
2101
AE TABLE
2102
AF TABLE
2103
BD TABLE
2104
BE TABLE
2105
LINK DOWN
BF TABLE
2106
2100
CD TABLE
2107
CE TABLE
2108
CF TABLE
2109

FIG. 21

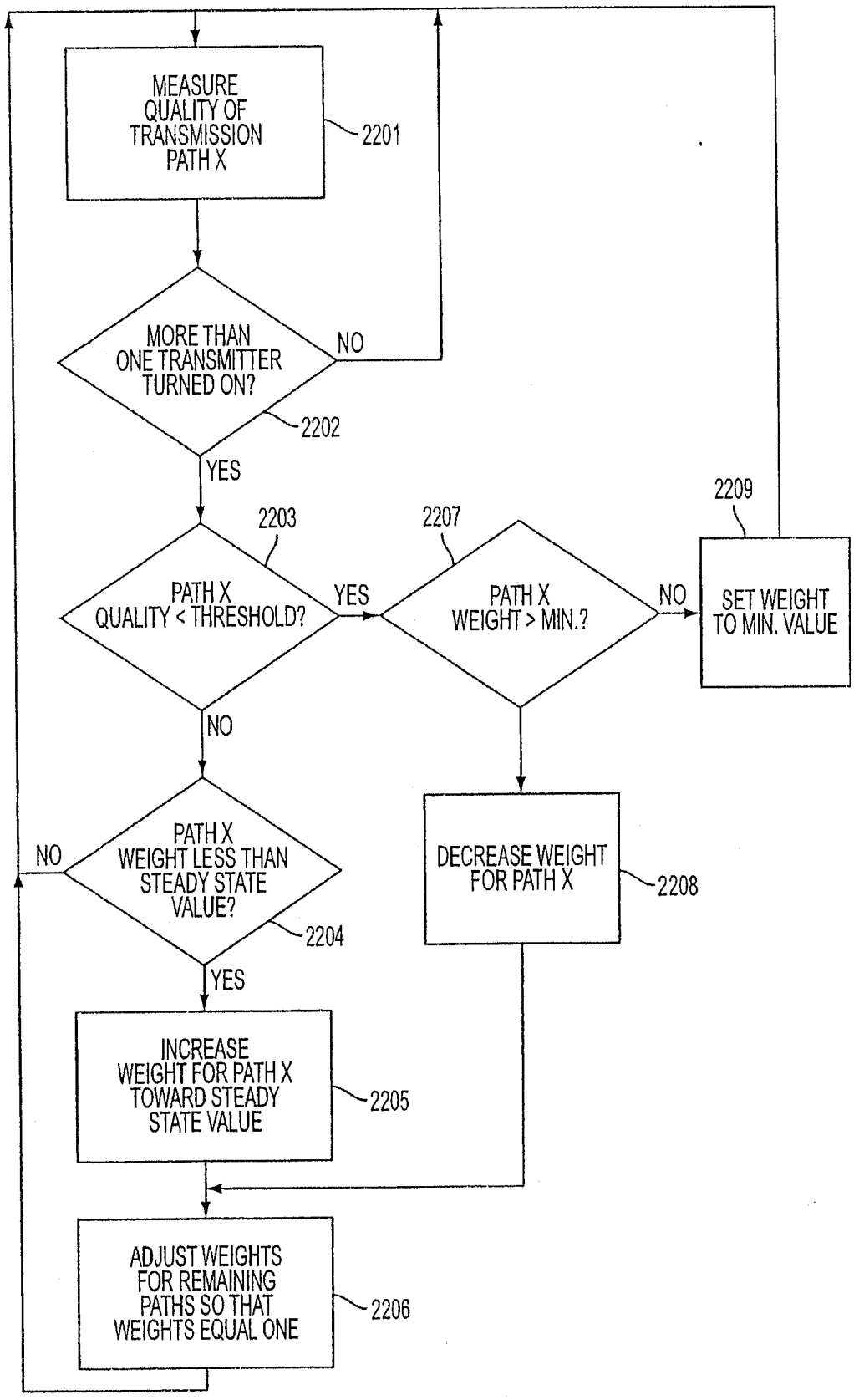

MEASURE QUALITY OF TRANSMISSION PATH X
2201
MORE THAN ONE TRANSMITTER TURNED ON?
NO
2202
YES
2203
PATH X QUALITY < THRESHOLD?
YES
2207
PATH X WEIGHT > MIN.?
NO
2209
SET WEIGHT TO MIN. VALUE
NO
PATH X WEIGHT LESS THAN STEADY STATE VALUE?
NO
2204
YES
DECREASE WEIGHT FOR PATH X
2208
INCREASE WEIGHT FOR PATH X TOWARD STEADY STATE VALUE
2205
ADJUST WEIGHTS FOR REMAINING PATHS SO THAT WEIGHTS EQUAL ONE
2206

FIG. 22A

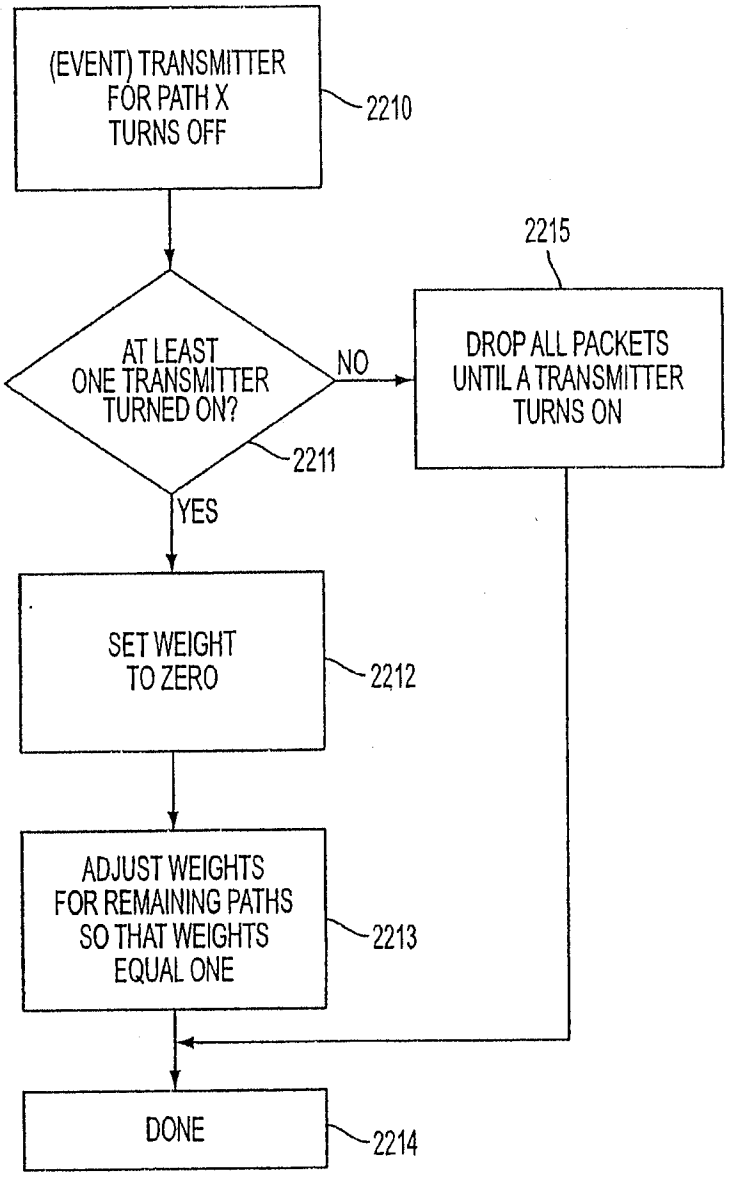

(EVENT) TRANSMITTER FOR PATH X TURNS OFF
2210
AT LEAST ONE TRANSMITTER TURNED ON?
NO
2211
YES
2215
DROP ALL PACKETS UNTIL A TRANSMITTER TURNS ON
SET WEIGHT TO ZERO
2212
ADJUST WEIGHTS FOR REMAINING PATHS SO THAT WEIGHTS EQUAL ONE
2213
DONE
2214

FIG. 22B

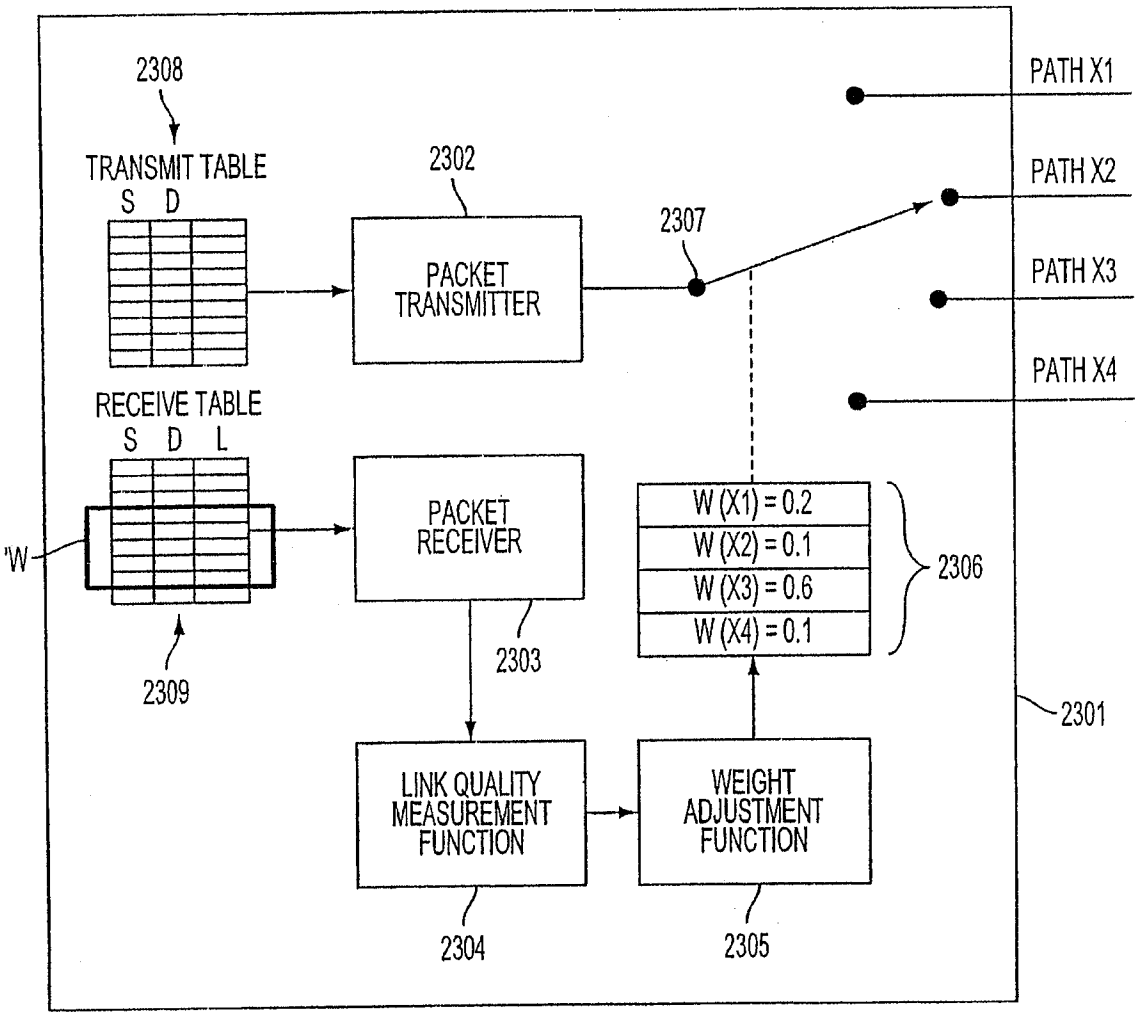

2308
TRANSMIT TABLE
S D
2302
PACKET TRANSMITTER
2307
PATH X1
PATH X2
PATH X3
PATH X4
RECEIVE TABLE
S D L
'W
PACKET RECEIVER
W (X1) = 0.2
W (X2) = 0.1
W (X3) = 0.6
W (X4) = 0.1
2306
2309
2303
2301
LINK QUALITY MEASUREMENT FUNCTION
WEIGHT ADJUSTMENT FUNCTION
2304
2305

FIG. 23

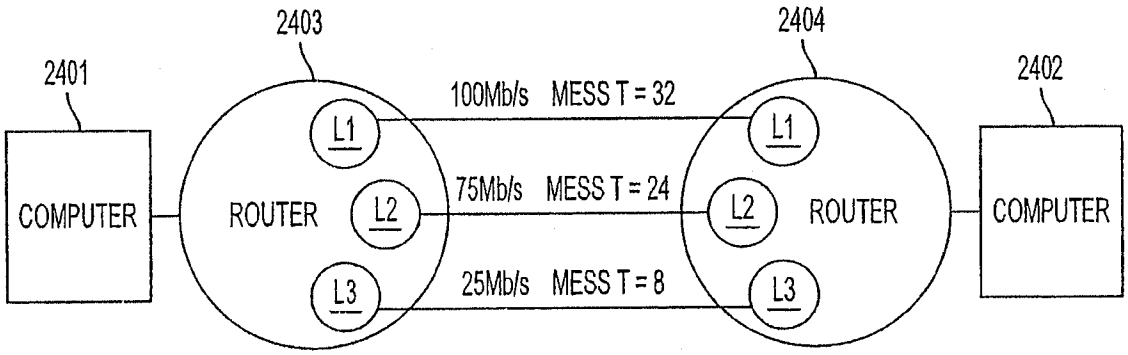

2401
2403
2404
2402
COMPUTER
ROUTER
L1
L2
L3
100Mb/s MESS T = 32
75Mb/s MESS T = 24
25Mb/s MESS T = 8
L1
L2
L3
ROUTER
COMPUTER

FIG. 24

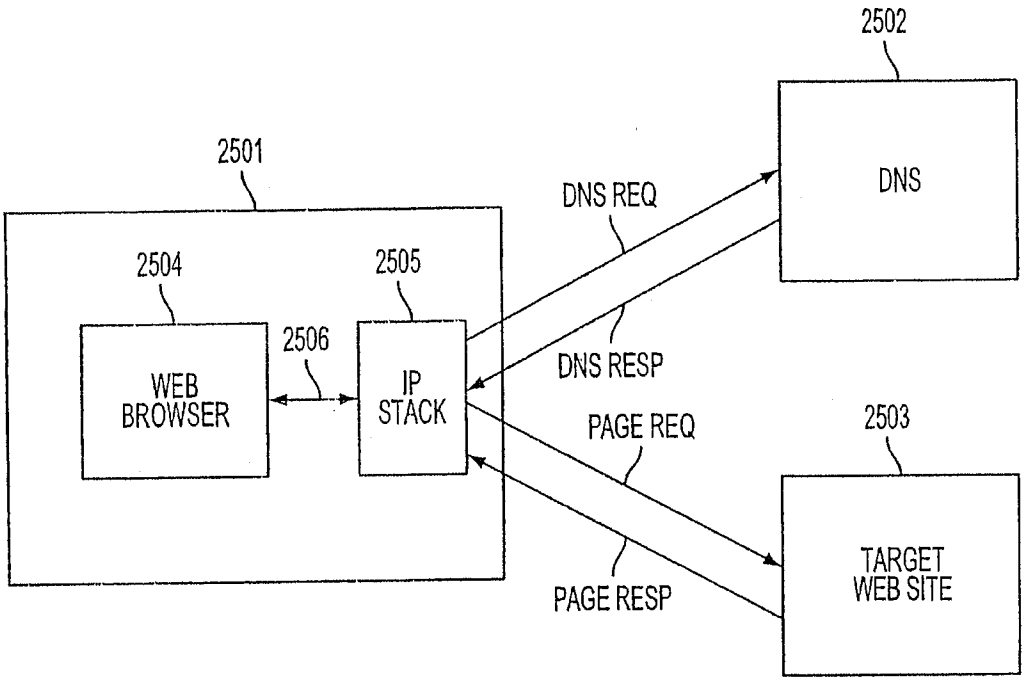


FIG. 25
(PRIOR ART)

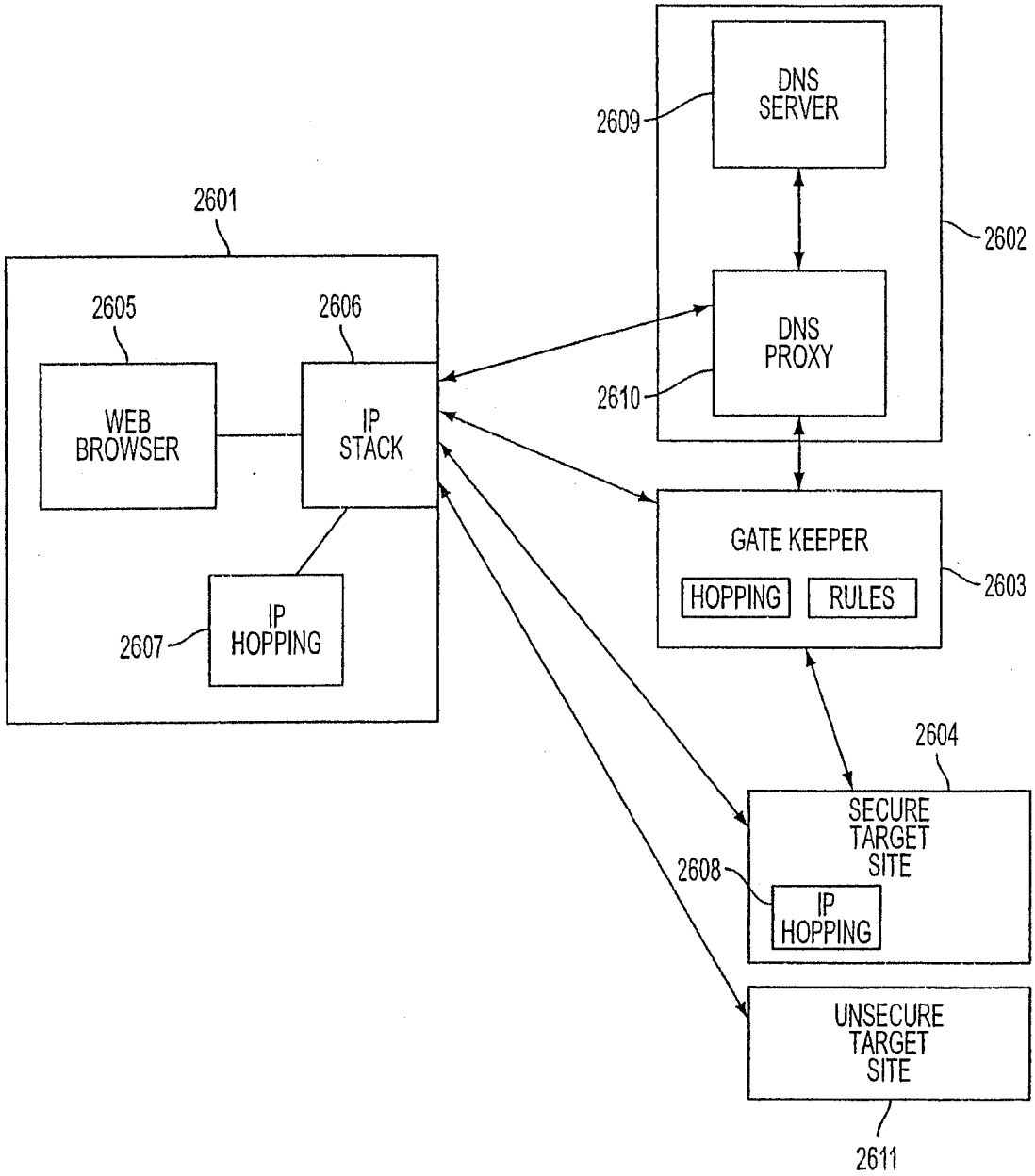

DNS SERVER
2609
2602
2601
2605
2606
DNS PROXY
2610
WEB BROWSER
IP STACK
GATE KEEPER
HOPPING
RULES
2603
IP HOPPING
2607
2604
SECURE TARGET SITE
2608
IP HOPPING
UNSECURE TARGET SITE
2611

FIG. 26

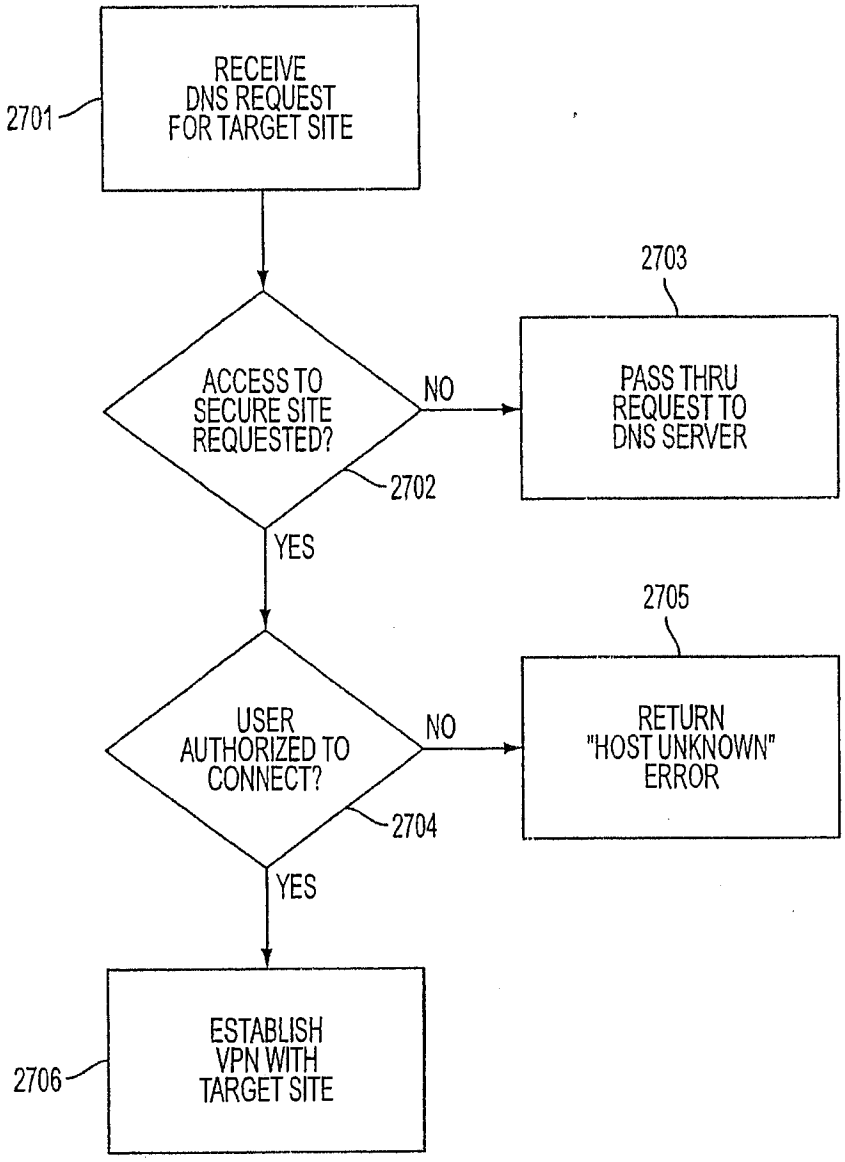

RECEIVE DNS REQUEST FOR TARGET SITE
2701
ACCESS TO SECURE SITE REQUESTED?
2702
NO
2703
PASS THRU REQUEST TO DNS SERVER
YES
USER AUTHORIZED TO CONNECT?
2704
NO
2705
RETURN "HOST UNKNOWN" ERROR
YES
ESTABLISH VPN WITH TARGET SITE
2706

FIG. 27

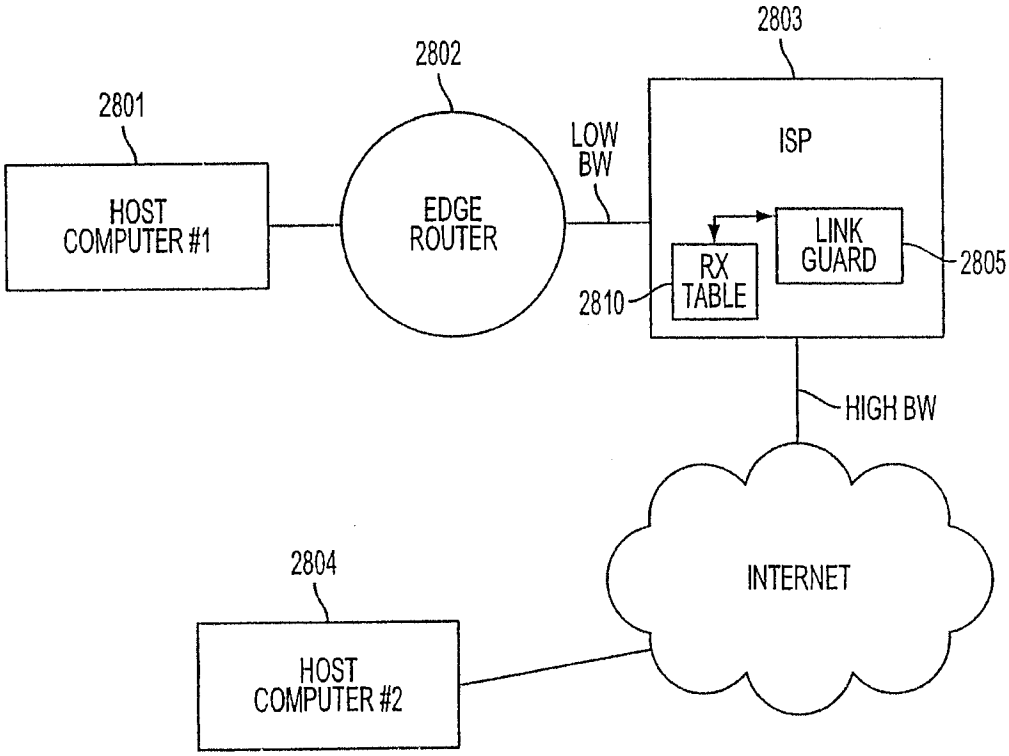

2803
2802
2801
ISP
LOW
BW
HOST
COMPUTER #1
EDGE
ROUTER
LINK
GUARD
2805
RX
TABLE
2810
HIGH BW
INTERNET
2804
HOST
COMPUTER #2

FIG. 28

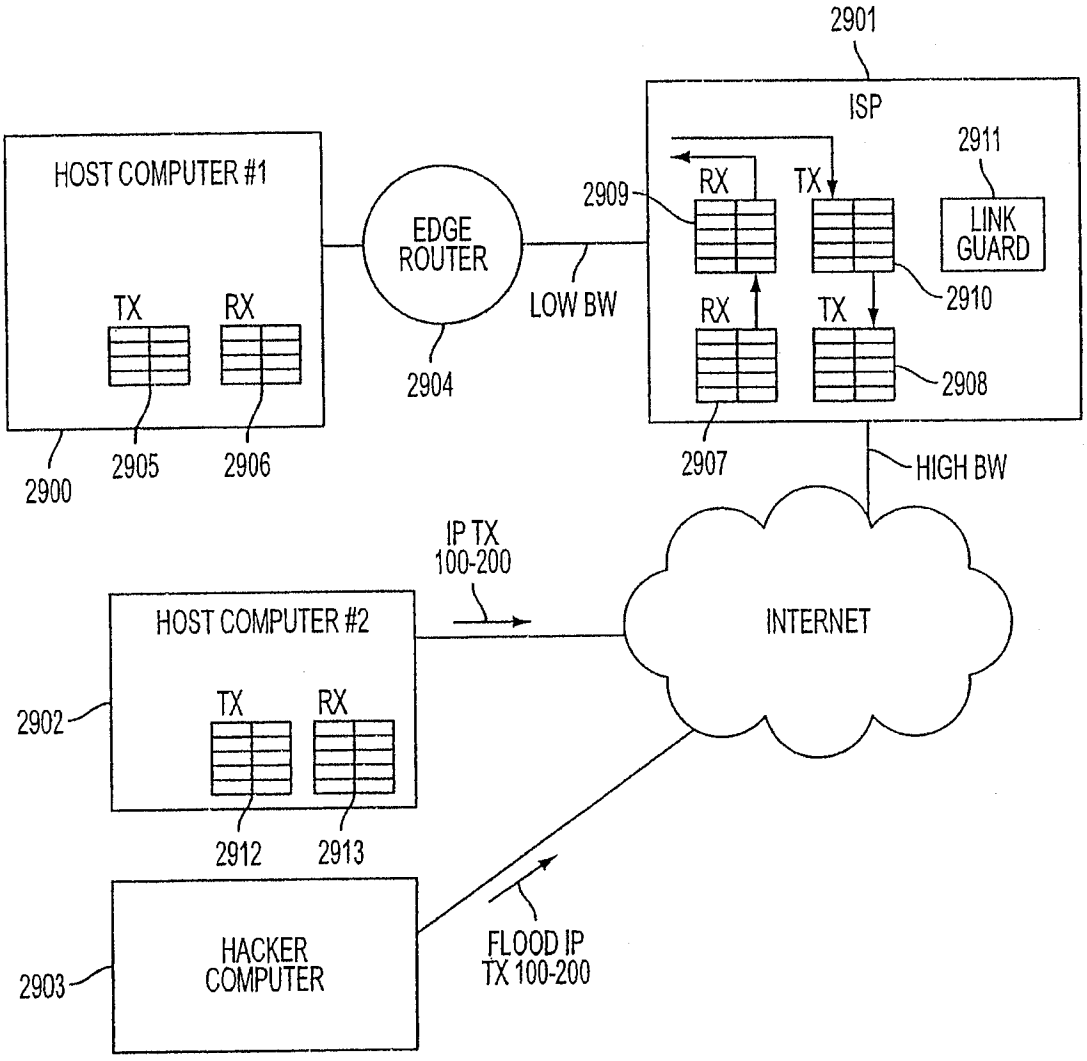

2901
ISP
HOST COMPUTER #1
EDGE ROUTER
2909
RX
TX
2911
LINK GUARD
2910
LOW BW
RX
TX
2908
2904
2907
HIGH BW
TX
RX
2900
2905
2906
IP TX 100-200
INTERNET
HOST COMPUTER #2
2902
TX
RX
2912
2913
HACKER COMPUTER
2903
FLOOD IP TX 100-200

FIG. 29

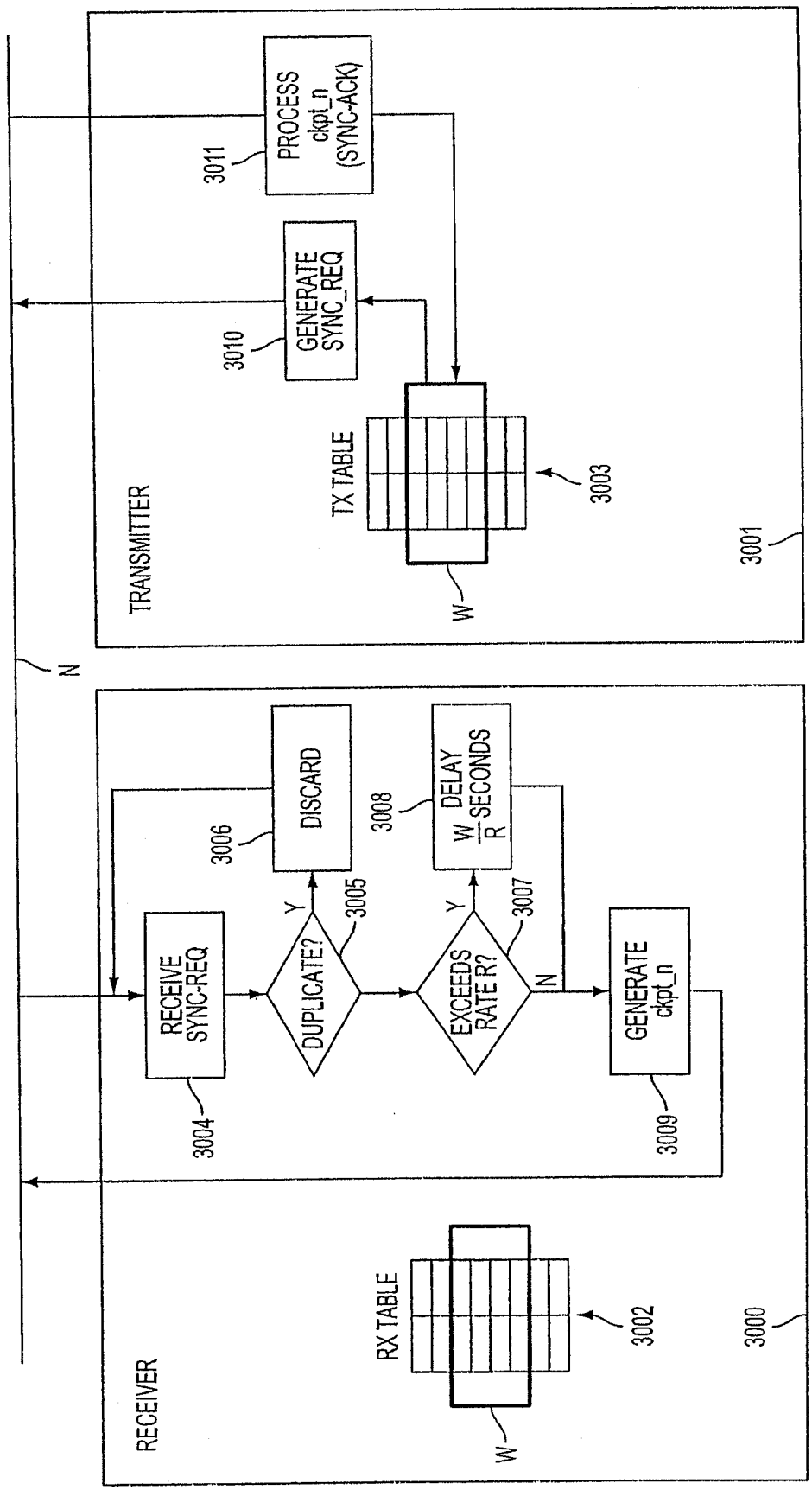

TRANSMITTER
3001
PROCESS ckpt_n (SYNC-ACK)
3011
GENERATE SYNC_REQ
3010
TX TABLE
3003
W
N
RECEIVER
3000
RECEIVE SYNC-REQ
3004
DUPLICATE?
3005
Y
DISCARD
3006
EXCEEDS RATE R?
3007
Y
N
DELAY W/R SECONDS
3008
GENERATE ckpt_n
3009
RX TABLE
3002
W

FIG. 30

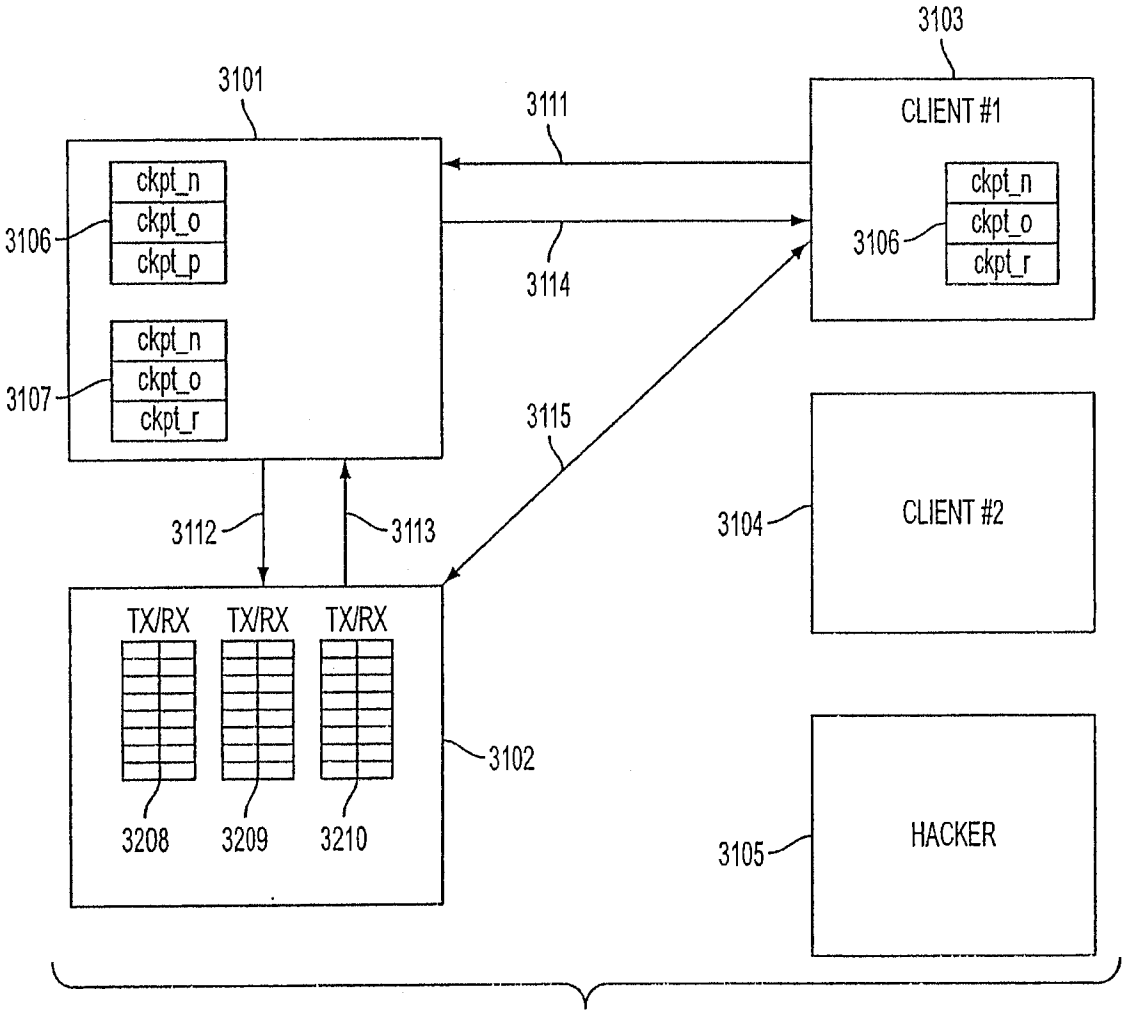

3103
3101
3111
CLIENT #1
ckpt_n
ckpt_o
ckpt_p
3106
ckpt_n
ckpt_o
ckpt_r
3106
3114
ckpt_n
ckpt_o
ckpt_r
3107
3115
3112
3113
3104
CLIENT #2
TX/RX
TX/RX
TX/RX
3102
3208
3209
3210
3105
HACKER

FIG. 31

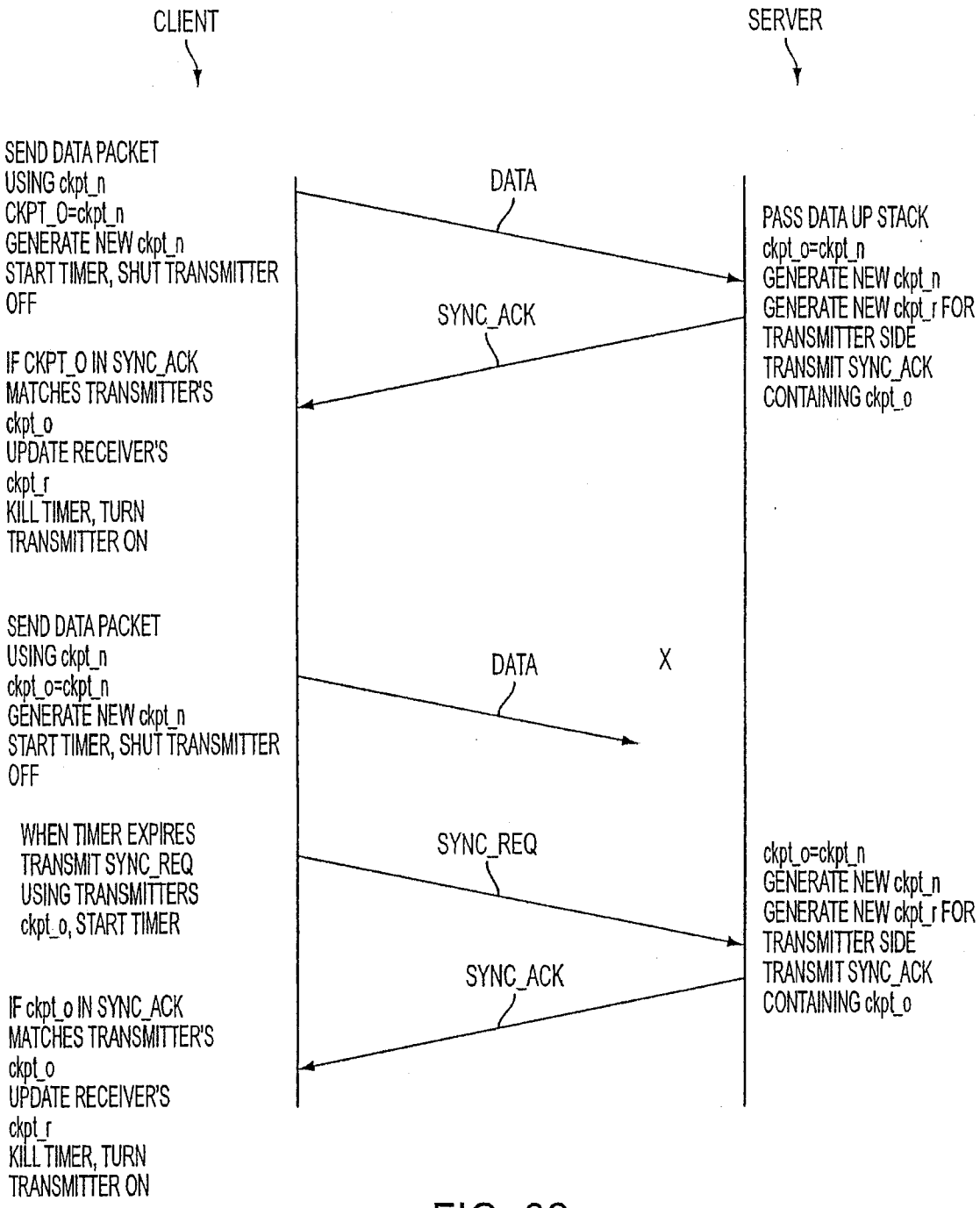

CLIENT
SERVER
SEND DATA PACKET
USING ckpt_n
CKPT_O=ckpt_n
GENERATE NEW ckpt_n
START TIMER, SHUT TRANSMITTER OFF
DATA
PASS DATA UP STACK
ckpt_o=ckpt_n
GENERATE NEW ckpt_n
GENERATE NEW ckpt_r FOR TRANSMITTER SIDE
TRANSMIT SYNC_ACK CONTAINING ckpt_o
SYNC_ACK
IF CKPT_O IN SYNC_ACK MATCHES TRANSMITTER'S ckpt_o
UPDATE RECEIVER'S ckpt_r
KILL TIMER, TURN TRANSMITTER ON
SEND DATA PACKET
USING ckpt_n
ckpt_o=ckpt_n
GENERATE NEW ckpt_n
START TIMER, SHUT TRANSMITTER OFF
DATA
X
WHEN TIMER EXPIRES
TRANSMIT SYNC_REQ
USING TRANSMITTERS
ckpt_o, START TIMER
SYNC_REQ
ckpt_o=ckpt_n
GENERATE NEW ckpt_n
GENERATE NEW ckpt_r FOR TRANSMITTER SIDE
TRANSMIT SYNC_ACK CONTAINING ckpt_o
SYNC_ACK
IF ckpt_o IN SYNC_ACK MATCHES TRANSMITTER'S ckpt_o
UPDATE RECEIVER'S ckpt_r
KILL TIMER, TURN TRANSMITTER ON

FIG. 32

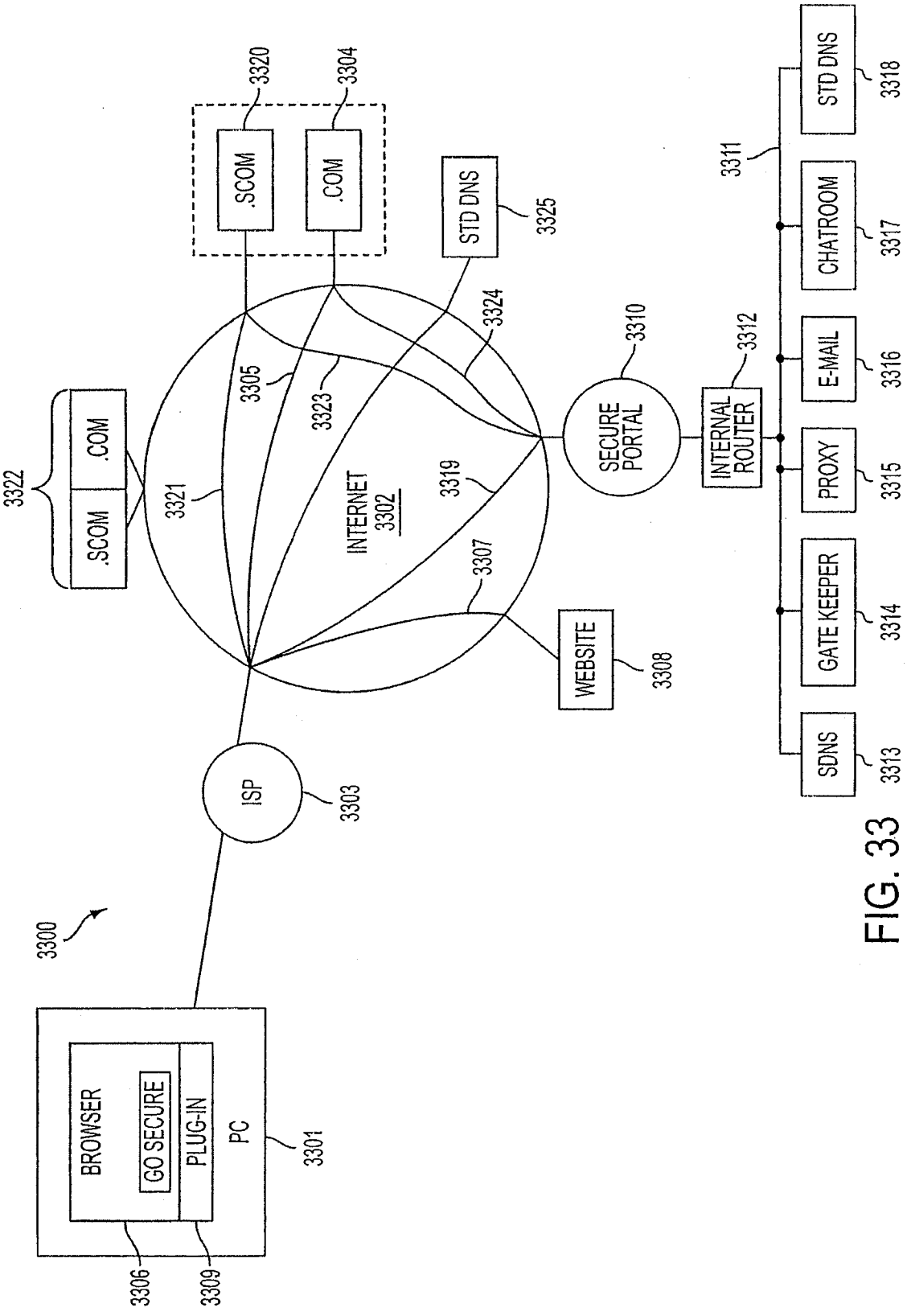

3300
BROWSER
GO SECURE
PLUG-IN
PC
3301
3306
3309
ISP
3303
INTERNET
3302
.SCOM
.COM
3322
3321
3320
3304
.SCOM
.COM
3305
3323
3324
STD DNS
3325
3319
3307
WEBSITE
3308
SECURE PORTAL
3310
INTERNAL ROUTER
3312
3311
STD DNS
3318
CHATROOM
3317
E-MAIL
3316
PROXY
3315
GATE KEEPER
3314
SDNS
3313

FIG. 33

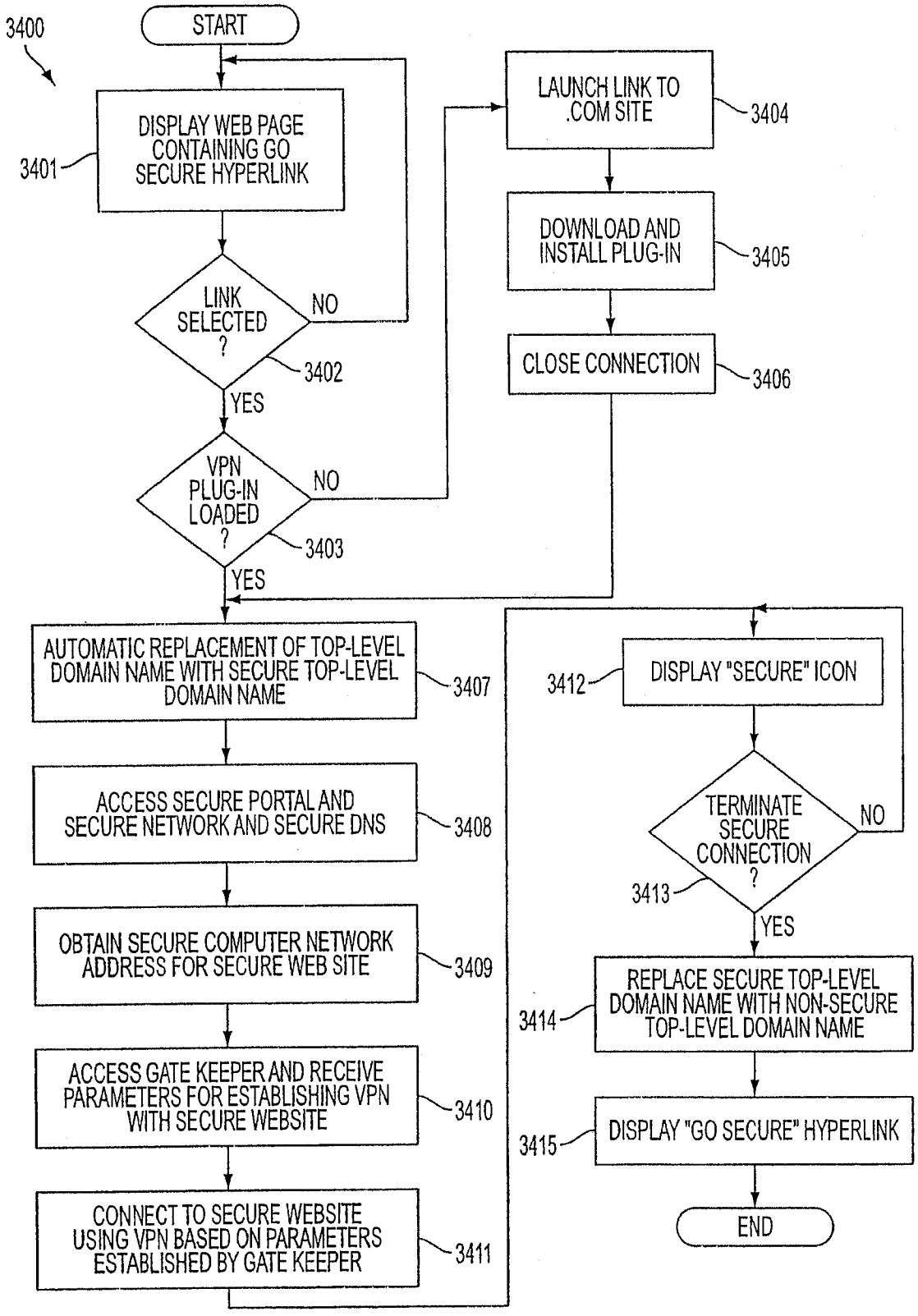

3400
START
DISPLAY WEB PAGE CONTAINING GO SECURE HYPERLINK
3401
LINK SELECTED ?
NO
3402
YES
VPN PLUG-IN LOADED ?
NO
3403
YES
LAUNCH LINK TO .COM SITE
3404
DOWNLOAD AND INSTALL PLUG-IN
3405
CLOSE CONNECTION
3406
AUTOMATIC REPLACEMENT OF TOP-LEVEL DOMAIN NAME WITH SECURE TOP-LEVEL DOMAIN NAME
3407
ACCESS SECURE PORTAL AND SECURE NETWORK AND SECURE DNS
3408
OBTAIN SECURE COMPUTER NETWORK ADDRESS FOR SECURE WEB SITE
3409
ACCESS GATE KEEPER AND RECEIVE PARAMETERS FOR ESTABLISHING VPN WITH SECURE WEBSITE
3410
CONNECT TO SECURE WEBSITE USING VPN BASED ON PARAMETERS ESTABLISHED BY GATE KEEPER
3411
3412
DISPLAY "SECURE" ICON
TERMINATE SECURE CONNECTION ?
NO
3413
YES
REPLACE SECURE TOP-LEVEL DOMAIN NAME WITH NON-SECURE TOP-LEVEL DOMAIN NAME
3414
DISPLAY "GO SECURE" HYPERLINK
3415
END

FIG. 34

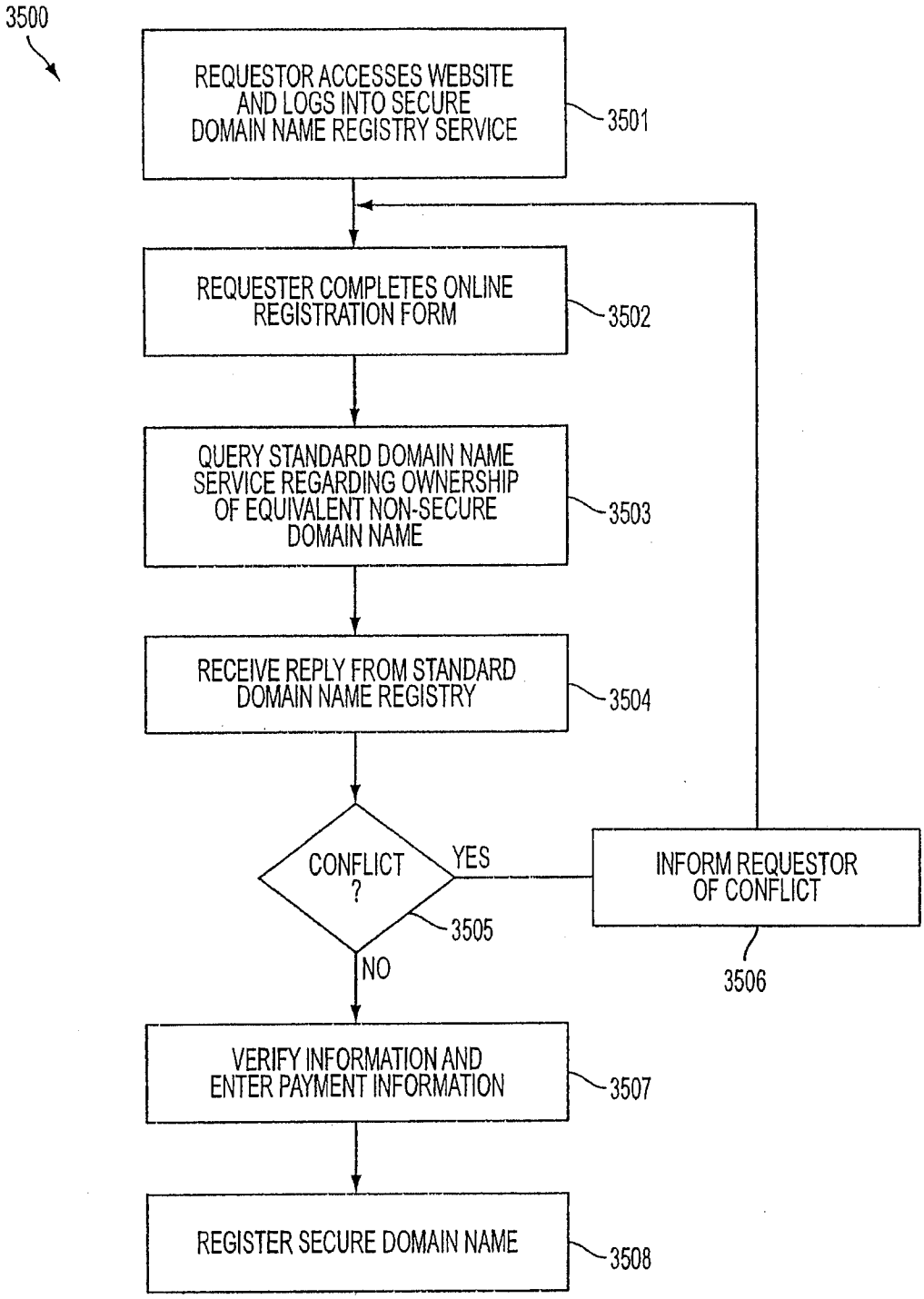

3500
REQUESTOR ACCESSES WEBSITE AND LOGS INTO SECURE DOMAIN NAME REGISTRY SERVICE
3501
REQUESTER COMPLETES ONLINE REGISTRATION FORM
3502
QUERY STANDARD DOMAIN NAME SERVICE REGARDING OWNERSHIP OF EQUIVALENT NON-SECURE DOMAIN NAME
3503
RECEIVE REPLY FROM STANDARD DOMAIN NAME REGISTRY
3504
CONFLICT ?
YES
3505
NO
INFORM REQUESTOR OF CONFLICT
3506
VERIFY INFORMATION AND ENTER PAYMENT INFORMATION
3507
REGISTER SECURE DOMAIN NAME
3508

FIG. 35

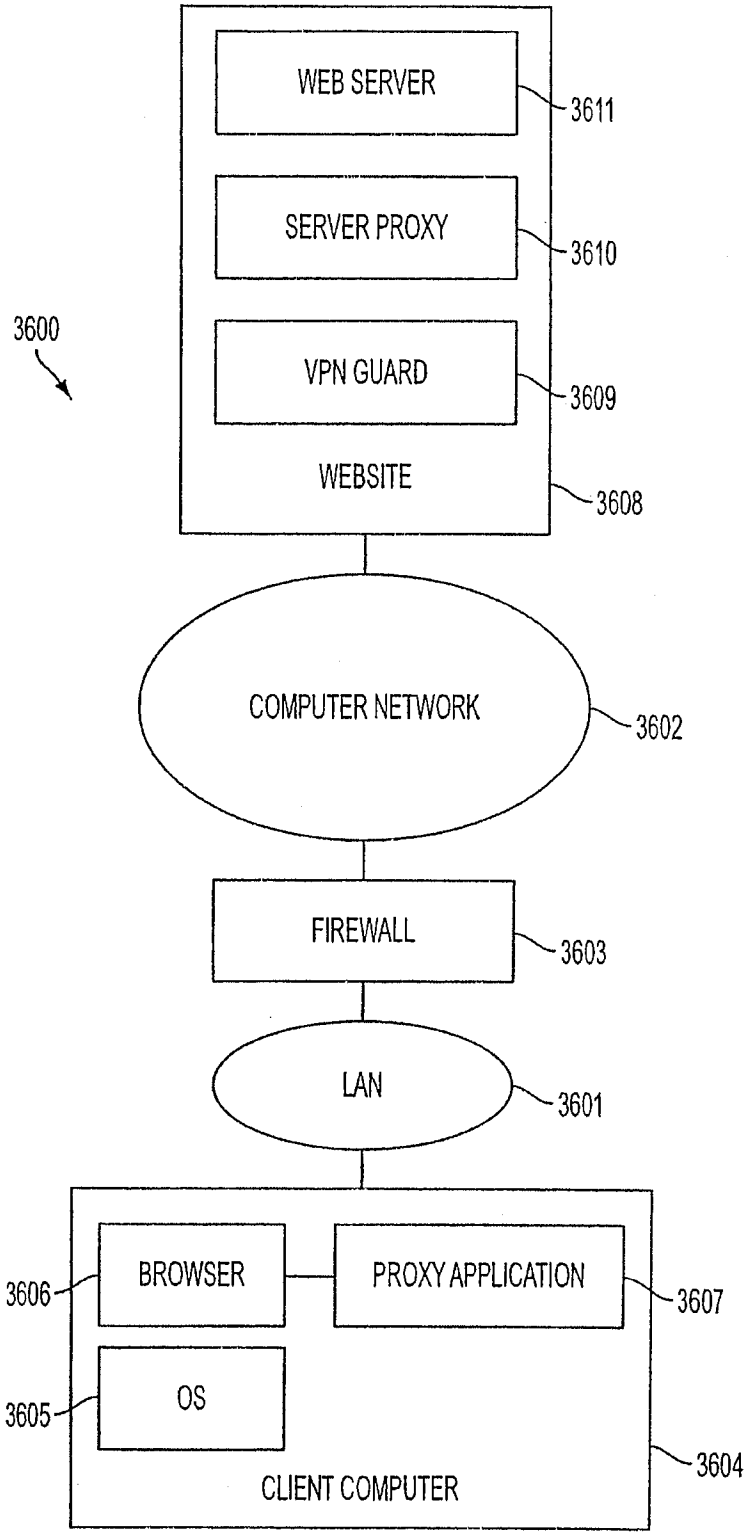

3600
WEB SERVER
3611
SERVER PROXY
3610
VPN GUARD
3609
WEBSITE
3608
COMPUTER NETWORK
3602
FIREWALL
3603
LAN
3601
BROWSER
PROXY APPLICATION
3606
3607
OS
3605
CLIENT COMPUTER
3604

FIG. 36

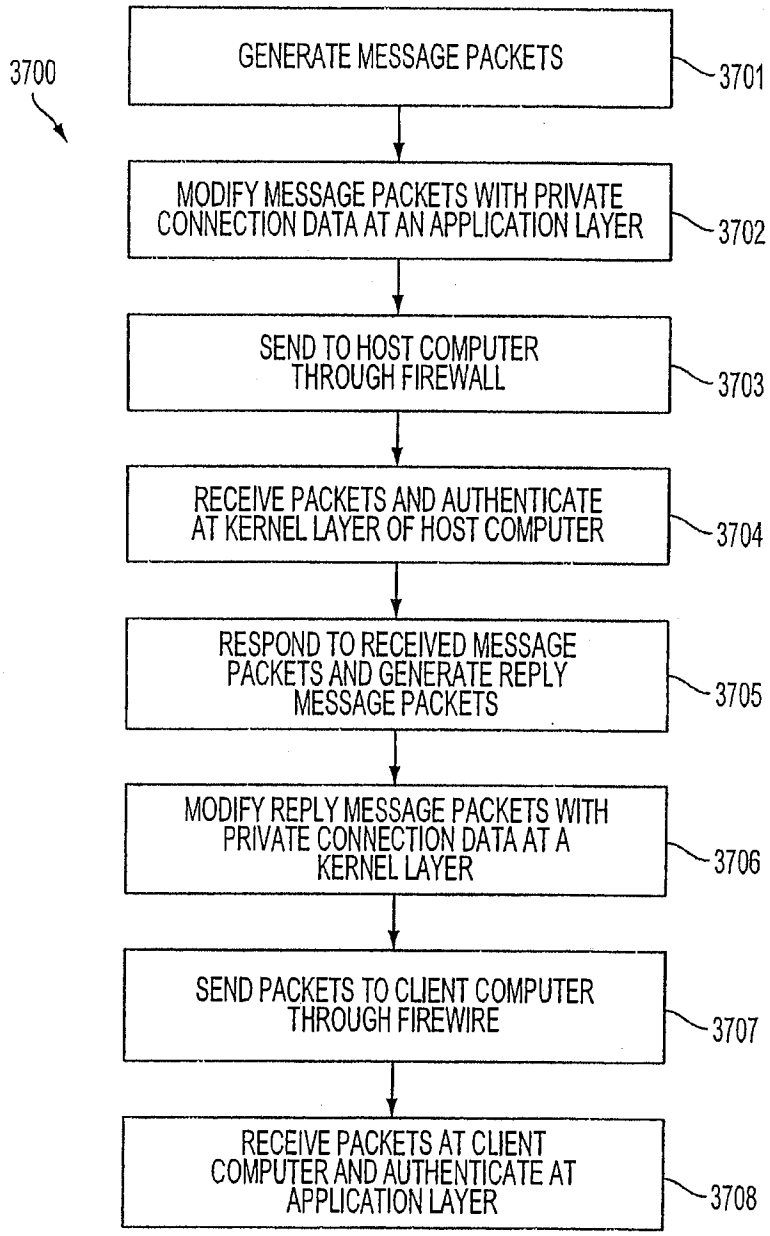

3700
GENERATE MESSAGE PACKETS
3701
MODIFY MESSAGE PACKETS WITH PRIVATE CONNECTION DATA AT AN APPLICATION LAYER
3702
SEND TO HOST COMPUTER THROUGH FIREWALL
3703
RECEIVE PACKETS AND AUTHENTICATE AT KERNEL LAYER OF HOST COMPUTER
3704
RESPOND TO RECEIVED MESSAGE PACKETS AND GENERATE REPLY MESSAGE PACKETS
3705
MODIFY REPLY MESSAGE PACKETS WITH PRIVATE CONNECTION DATA AT A KERNEL LAYER
3706
SEND PACKETS TO CLIENT COMPUTER THROUGH FIREWIRE
3707
RECEIVE PACKETS AT CLIENT COMPUTER AND AUTHENTICATE AT APPLICATION LAYER
3708

FIG. 37

Electronic Acknowledgement Receipt

EFS ID:	11704565
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Jessica Brown
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	23-DEC-2011
Filing Date:	
Time Stamp:	19:34:27
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	151TransmittalReplacementDrawings.pdf	22744 43c2a38200396598e29fa4166a36885f560af057	no	1

Warnings:	
Information:	

2	Drawings-only black and white line drawings	151ReplacementDrawings.pdf	549449 2419b3a118e466c2173663ed94012ba0f35701de	no	40

Warnings:	
Information:	
Total Files Size (in bytes):	572193

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronic Acknowledgement Receipt

EFS ID:	11703565
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Jessica Brown
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	23-DEC-2011
Filing Date:	
Time Stamp:	16:41:42
Application Type:	Utility under 35 USC 111(a)

Adjustment date: 01/09/2012 MTEKLEMI
12/27/2011 INTEFSW 00003068 501133 13336790
05 FC:1081 310.00 CR

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$7270
RAM confirmation Number	3068
Deposit Account	501133
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 13/336,790

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	380
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	620
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	250
TOTAL CLAIMS (37 CFR 1.16(i))	28 minus 20 =	* 8			OR	x 60 =	480
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2 minus 3 =	*				x 250 =	0.00
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	1730

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/336,790	12/23/2011	2447	2030	77580-151(VRNK-1CP3CNFT1)	28	2

CONFIRMATION NO. 6217

23630
McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

FILING RECEIPT

Date Mailed: 01/13/2012

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Victor Larson, Fairfax, VA;
Robert Dunham Short III, Leesburg, VA;
Edmond Colby Munger, Crownsville, MD;
Michael Williamson, South Riding, VA;

Assignment For Published Patent Application

VIRNETX, INC., Scotts Valley, CA

Power of Attorney: The patent practitioners associated with Customer Number 23630

Domestic Priority data as claimed by applicant

This application is a CON of 13/049,552 03/16/2011
which is a CON of 11/840,560 08/17/2007 PAT 7921211
which is a CON of 10/714,849 11/18/2003 PAT 7418504
which is a CON of 09/558,210 04/26/2000 ABN
which is a CIP of 09/504,783 02/15/2000 PAT 6502135
which is a CIP of 09/429,643 10/29/1999 PAT 7010604
which claims benefit of 60/106,261 10/30/1998
and claims benefit of 60/137,704 06/07/1999

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)

If Required, Foreign Filing License Granted: 01/09/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/336,790**

Petitioner Apple Inc. - Exhibit 1002, p. 206

Projected Publication Date: To Be Determined - pending completion of Corrected Papers

Non-Publication Request: No

Early Publication Request: No

Title

SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

Preliminary Class

709

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

Petitioner Apple Inc. - Exhibit 1002, p. 207

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/336,790	12/23/2011	Victor Larson	77580-151(VRNK-1CP3CNFT1)

CONFIRMATION NO. 6217

23630
McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

FORMALITIES LETTER

OC000000051953355

Date Mailed: 01/13/2012

NOTICE TO FILE CORRECTED APPLICATION PAPERS

Filing Date Granted

An application number and filing date have been accorded to this application. The application is informal since it does not comply with the regulations for the reason(s) indicated below. Applicant is given TWO MONTHS from the date of this Notice within which to correct the informalities indicated below. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

The required item(s) identified below must be timely submitted to avoid abandonment:

- A replacement abstract not exceeding 150 words in length and commencing on a separate sheet in compliance with 37 CFR 1.72(b) and 37 CFR 1.121 is required.

Applicant is cautioned that correction of the above items may cause the specification and drawings page count to exceed 100 pages. If the specification and drawings exceed 100 pages, applicant will need to submit the required application size fee.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/tpetros/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Petitioner Apple Inc. - Exhibit 1002, p. 209

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/336,790	12/23/2011	Victor Larson	77580-151(VRNK-1CP3CNFT1)

CONFIRMATION NO. 6217

23630
McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

POA ACCEPTANCE LETTER

OC000000051903551

Date Mailed: 01/13/2012

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 12/23/2011.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/tchaka/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Docket No.: 77580-151(VRNK-1CP3CNFT1) **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Customer Number: 23630
LARSON, Victor et al.	:	Confirmation Number: 6217
Application No.: 13/336,790	:	Group Art Unit: 2447
Filed: December 23, 2011	:	Examiner: Unknown

For: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this correspondence is being electronically-transmitted to the United States Patent and Trademark Office on **January 19, 2012**

/Jessica Brown/
Jessica Brown

RESPONSE TO NOTICE TO FILE CORRECTED APPLICATION PAPERS MAILED JANUARY 13, 2012

Mail Stop MISSING PARTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir/Madam:

In response to the Notice to File Corrected Application Papers, dated January 13, 2012 submitted herewith are the following for filing in the above-referenced application:

1. Copy of Notice to File Corrected Application Papers; and
2. Replacement Abstract not exceeding 150 words in length and commencing on a separate sheet.

Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-1133 and please credit any excess fees to such deposit account, referencing attorney docket no. 77580-151(VRNK-1CP3CNFT1).

Petitioner Apple Inc. - Exhibit 1002, p. 211

It is requested that an updated, corrected official filing receipt now be issued.

Respectfully submitted,
McDERMOTT WILL & EMERY LLP

/Toby H. Kusmer/

Toby H. Kusmer, P.C., Reg. No. 26,418

600 13th Street, N.W.
Washington, D.C. 20005-3096
Phone: 617.535.4065
Facsimile: 617.535.3800
Date: January 19, 2012

Please recognize our Customer No. 23630 as our correspondence address.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/336,790	12/23/2011	Victor Larson	77580-151(VRNK-1CP3CNFT1)

CONFIRMATION NO. 6217

23630
McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

FORMALITIES LETTER

OC000000051953355

Date Mailed: 01/13/2012

NOTICE TO FILE CORRECTED APPLICATION PAPERS

Filing Date Granted

An application number and filing date have been accorded to this application. The application is informal since it does not comply with the regulations for the reason(s) indicated below. Applicant is given TWO MONTHS from the date of this Notice within which to correct the informalities indicated below. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

The required item(s) identified below must be timely submitted to avoid abandonment:

- A replacement abstract not exceeding 150 words in length and commencing on a separate sheet in compliance with 37 CFR 1.72(b) and 37 CFR 1.121 is required.

Applicant is cautioned that correction of the above items may cause the specification and drawings page count to exceed 100 pages. If the specification and drawings exceed 100 pages, applicant will need to submit the required application size fee.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/tpetros/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Petitioner Apple Inc. - Exhibit 1002, p. 213

REPLACEMENT ABSTRACT

A network device comprises a storage device storing an application program for a secure communications service and at least one processor. The processor is configured to execute the application program enabling the network device to (a) send a request to look up a network address of a second network device based on an identifier associated with the second network device; (b) receive an indication that the second network device is available for the secure communications service, the indication including the requested network address of the second network device and provisioning information for a virtual private network communication link; (c) connect to the second network device, using the received network address of the second network device and the provisioning information for the virtual private network communication link; and (d) communicate with the second network device using the secure communications service via the virtual private network communication link.

Electronic Acknowledgement Receipt

EFS ID:	11879366
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Jessica Brown
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	19-JAN-2012
Filing Date:	23-DEC-2011
Time Stamp:	19:55:54
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		151ResponseNTFCAP.pdf	709589 22b66c3b12d8f9d09425614ef601e03de41ca59b	yes	4

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Applicant Response to Pre-Exam Formalities Notice	1	3
	Abstract	4	4
Warnings:			
Information:			
	Total Files Size (in bytes):	709589	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 13/336,790

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	380
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	620
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	250
TOTAL CLAIMS (37 CFR 1.16(i))	28 minus 20 =	* 8			OR	x 60 =	480
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2 minus 3 =	*				x 250 =	0.00
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	1730

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/336,790	12/23/2011	2447	2030	77580-151(VRNK-1CP3CNFT1)	28	2

CONFIRMATION NO. 6217

UPDATED FILING RECEIPT

23630
McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

OC000000052204572

Date Mailed: 01/27/2012

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Victor Larson, Fairfax, VA;
Robert Dunham Short III, Leesburg, VA;
Edmond Colby Munger, Crownsville, MD;
Michael Williamson, South Riding, VA;

Assignment For Published Patent Application

VIRNETX, INC., Scotts Valley, CA

Power of Attorney: The patent practitioners associated with Customer Number 23630

Domestic Priority data as claimed by applicant

This application is a CON of 13/049,552 03/16/2011
which is a CON of 11/840,560 08/17/2007 PAT 7921211
which is a CON of 10/714,849 11/18/2003 PAT 7418504
which is a CON of 09/558,210 04/26/2000 ABN
which is a CIP of 09/504,783 02/15/2000 PAT 6502135
which is a CIP of 09/429,643 10/29/1999 PAT 7010604
which claims benefit of 60/106,261 10/30/1998
and claims benefit of 60/137,704 06/07/1999

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)

If Required, Foreign Filing License Granted: 01/09/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/336,790**

Petitioner Apple Inc. - Exhibit 1002, p. 218

Projected Publication Date: 05/03/2012

Non-Publication Request: No

Early Publication Request: No

Title

SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

Preliminary Class

709

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

Petitioner Apple Inc. - Exhibit 1002, p. 219

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/336,790	12/23/2011	Victor Larson	77580-151(VRNK-1CP3CNFT1)	6217

23630 7590 02/13/2012

McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

EXAMINER	
HWANG, JOON H	

ART UNIT	PAPER NUMBER
2447	

NOTIFICATION DATE	DELIVERY MODE
02/13/2012	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mweipdocket@mwe.com

Doc Code: TRACK1.GRANT

Decision Granting Request for Prioritized Examination (Track I or After RCE)	Application No.: 13336790

1. THE REQUEST FILED 12/23/2011 IS **GRANTED.**

The above-identified application has met the requirements for prioritized examination

A. x☐ for an original nonprovisional application (Track I).

B. ☐ for an application undergoing continued examination (RCE).

2. **The above-identified application will undergo prioritized examination.** The application will be accorded special status throughout its entire course of prosecution until one of the following occurs:

A. filing a **petition for extension of time** to extend the time period for filing a reply;

B. filing an **amendment to amend the application to contain more than four independent claims, more than thirty total claims**, or a multiple dependent claim;

C. filing a **request for continued examination**;

D. filing a notice of appeal;

E. filing a request for suspension of action;

F. mailing of a notice of allowance;

G. mailing of a final Office action;

H. completion of examination as defined in 37 CFR 41.102; or

I. abandonment of the application.

Telephone inquiries with regard to this decision should be directed to Mano Padmanabhan at 571-272-4210. In his/her absence, calls may be directed to Kakali Chaki, 571-272-3719.

/Mano Padmanabhan/ Supervisory Patent Examiner, AU2188

Petitioner Apple Inc. - Exhibit 1002, p. 222

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/336,790	12/23/2011	Victor Larson	77580-151(VRNK-1CP3CNFT1)	6217

23630 7590 03/02/2012

McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

EXAMINER	
LIM, KRISNA	
ART UNIT	PAPER NUMBER
2453	

NOTIFICATION DATE	DELIVERY MODE
03/02/2012	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mweipdocket@mwe.com

Office Action Summary	Application No.	Applicant(s)	
	13/336,790	LARSON ET AL.	
	Examiner	Art Unit	
	KRISNA LIM	2453	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 January 2012*.

2a)☐ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-28* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-28* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

1. Claims 1-28 are presented for examination.'

The applicant's oath/declaration has been reviewed by the examiner and is found to conform to the requirements prescribed in 37 C.F.R. 1.63.

2. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

3. Claims 1-28 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-17 of U.S. Patent No. 6,502,135. Although the conflicting claims are not identical, they are not patentably distinct from

each other because they are directed to a network device (a domain name service system) configured to be connected to a secure communication network using the received look up network address of a second network device based on an identifier associated with the second network device and the information for a virtual network address. The difference is a variation and clarification of the claim languages. For example, the current application clearly cites the storage device for storing application program for a secure communications service and a processor for executing the application program, and using an identifier associated with the second network device to look up for a second network device. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to recognize that such using of storage device for storing the application program and the processor for executing the application program are well known in the art and it is not patentably distinguishable.

4. Claims 1-28 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 3-7, 13-16 and 33-40 of U.S. Patent No. 7,188,180. Although the conflicting claims are not identical, they are not patentably distinct from each other because they are directed to a network device (a domain name service system) configured to be connected to a secure communication network using the received look up network address of a second network device based on an identifier associated with the second network device and the information for a virtual network address. The difference is a variation and clarification of the claim languages. For example, the current application clearly cites the storage device for storing application program for a secure communications service and a processor for executing the application program, and using an identifier associated with the second network device to look up for a second network device. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to recognize that such using of storage device for storing the application program and the processor for executing the application program are well known in the art and it is not patentably distinguishable.

5. Claims 1-28 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 8, 9, 12, 13, 14, 16, 17, and 23-33 of U.S. Patent No. 7,418,504. Although the conflicting claims are not identical, they are not patentably distinct from each other because they are directed to a network device (a domain name service system) configured to be connected to a secure communication network using the received look up network address of a second network device based on an identifier associated with the second network device and the information for a virtual network address. The difference is a variation and clarification of the claim languages. For example, the current application clearly cites the storage device for storing application program for a secure communications service and a processor for executing the application program, and using an identifier associated with the second network device to look up for a second network device. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to recognize that such using of storage device for storing the application program and the processor for executing the application program are well known in the art and it is not patentably distinguishable.

6. Claims 1-28 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 8-11 and 14-35 of U.S. Patent No. 7,921,211. Although the conflicting claims are not identical, they are not patentably distinct from each other because they are directed to a network device (a domain name service system) configured to be connected to a secure communication network using the received look up network address of a second network device based on an identifier associated with the second network device and the information for a virtual network address. The difference is a variation and clarification of the claim languages. For example, the current application clearly cites the storage device for storing application program for a secure communications service and a processor for executing the application program, and using an identifier associated with the second network device to look up for a second network device. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to recognize that such using of

storage device for storing the application program and the processor for executing the application program are well known in the art and it is not patentably distinguishable.

7. Claims 1-28 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-8, 10-13 and 17-18 of U.S. Patent No. 7,987,274. Although the conflicting claims are not identical, they are not patentably distinct from each other because they are directed to a network device (a domain name service system) configured to be connected to a secure communication network using the received look up network address of a second network device based on an identifier associated with the second network device and the information for a virtual network address. The difference is a variation and clarification of the claim languages. For example, the current application clearly cites the storage device for storing application program for a secure communications service and a processor for executing the application program, and using an identifier associated with the second network device to look up for a second network device. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to recognize that such using of storage device for storing the application program and the processor for executing the application program are well known in the art and it is not patentably distinguishable.

8. Claims 1-28 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-6, 8-9, and 14-22 of U.S. Patent No. 8,051,181. Although the conflicting claims are not identical, they are not patentably distinct from each other because they are directed to a network device (a domain name service system) configured to be connected to a secure communication network using the received look up network address of a second network device based on an identifier associated with the second network device and the information for a virtual network address. The difference is a variation and clarification of the claim languages. For example, the current application clearly cites the storage device for storing application

program for a secure communications service and a processor for executing the application program, and using an identifier associated with the second network device to look up for a second network device. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to recognize that such using of storage device for storing the application program and the processor for executing the application program are well known in the art and it is not patentably distinguishable.

9. Claims 1-28 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 14-20 and 26-39 of copending Application No. 13/080,680. Although the conflicting claims are not identical, they are not patentably distinct from each other because they are directed to a network device (a domain name service system) configured to be connected to a secure communication network using the received look up network address of a second network device based on an identifier associated with the second network device and the information for a virtual network address. The difference is a variation and clarification of the claim languages. For example, the current application clearly cites the storage device for storing application program for a secure communications service and a processor for executing the application program, and using an identifier associated with the second network device to look up for a second network device. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to recognize that such using of storage device for storing the application program and the processor for executing the application program are well known in the art and it is not patentably distinguishable.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

10. Claims 1-28 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-25 of copending Application No. 13/336,958. Although the conflicting claims are not identical, they are not patentably distinct from each other because they are directed to a network device comprising: a storage device storing an application program for a secure communication service; and at least one processor configured to execute the application program for the secure communications service so as to enable the network device to: a) send a request to look up ....; b) receive an indication ....; c) connect to the second network device …, and d) communicate ... via ... communication link. The difference is a variation and clarification of the claim languages. For example, the current application clearly cites that communicate with the second network device using the virtual private network communication link while the copending application 13/336,958 does not but instead citing that at least one of video data and audio data communicate with the second network device using only the secure communication link. Such variation and clarification are cited in the dependent claims and thus they are obvious and they are not patentably distinguishable.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

11. Claims 1-28 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-28 of copending Application No. 13/337,757. Although the conflicting claims are not identical, they are not patentably distinct from each other because they are directed to a network device using a virtual private network communication link to communication among network devices based a determination or indication. The difference is a variation and written style of the claim languages. For example, the current application uses an available indication of the second network device to communicate with while the

copending application uses an available determination of the second network device instead.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

12. Claims 1-28 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-28 of copending Application No. 13/339,257. Although the conflicting claims are not identical, they are not patentably distinct from each other because they are directed to a network device using a communication link to communication among network devices based a determination or indication. For example, the current application clearly cites that communicate with the second network device using the virtual private network communication link while the copending application does not but instead citing that at least one of video data and audio data communicate with the second network device using only the secure communication link. Such variation and clarification are cited in the dependent claims and thus they are obvious and they are not patentably distinguishable. Moreover, the difference is a variation and written style of the claim languages. For example, the current application uses an available indication of the second network device to communicate with while the copending application uses an available determination of the second network device instead. In addition, the current application clearly cites the storage device for storing application program for a secure communications service and a processor for executing the application program, and using an identifier associated with the second network device to look up for a second network device. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to recognize that such using of storage device for storing the application program and the processor for executing the application program are well known in the art and it is not patentably distinguishable.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

13. Claims 1-28 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-30 of copending Application No. 13/342,795. Although the conflicting claims are not identical, they are not patentably distinct from each other because they are directed to a network device using a communication link to communication among network devices based a determination or indication. For example, the current application clearly cites that communicate with the second network device (target device) using the virtual private network communication link while the copending application does not but instead citing that at least one of video data and audio data communicate with the target device using only the secure communication link. Such variation and clarification are cited in the dependent claims and thus they are obvious and they are not patentably distinguishable. Moreover, the difference is a variation and written style of the claim languages. In addition, the current application clearly cites the storage device for storing application program for a secure communications service and a processor for executing the application program, and using an identifier associated with the second network device to look up for a second network device. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to recognize that such using of storage device for storing the application program and the processor for executing the application program are well known in the art and it is not patentably distinguishable.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

14. Claims 1-28 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-30 of copending Application No. 13/343,465. Although the conflicting claims are not identical, they are not patentably distinct from each other because they are directed to a network device using a communication link to communication among network devices based a determination or indication. For example, the current application clearly cites that communicate with the second network device (target device) using the virtual private network communication link while the copending application does not but instead citing that at least one of video data and audio data communicate with the target device using the encrypted communication channel. Such variation and clarification are cited in the dependent claims and thus they are obvious and they are not patentably distinguishable. Moreover, the difference is a variation and written style of the claim languages. In addition, the current application clearly cites the storage device for storing application program for a secure communications service and a processor for executing the application program, and using an identifier associated with the second network device to look up for a second network device. It would have been obvious to one of ordinary skilled in the art at the time the invention was made to recognize that such using of storage device for storing the application program and the processor for executing the application program are well known in the art and it is not patentably distinguishable.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

15. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

16. Claims 1-28 are rejected under 35 U.S.C. § 103(a) as being unpatentable over VPN Overview and Aventail connect v3.1/v2.6 administrator's Guide References (hereafter VPN Overview and/or Aventail). Applicants submitted these papers in the parent application.

17. Aventail disclosed the invention substantially as claimed. Taking claims 1, 11, 12, 14, 15, 25, 27 and 28 as exemplary claims, the reference disclose a network device, comprising features of:

send a request to look up a network address of a second network device based on an identifier associated with the second network device (e.g., Window TCP/IP network application use WinSock to gain access to networks or the Internet ... and the application executes a DNS ... and requests a connection ..., see page 8 of Aventail);

connect to the second network device, using the received network address of the second network device and communicate with the second network device using the secure communications service via the network communication link (e.g., Aventail, Page 77- Depending on the security policy and the Aventail ExtraNet Server configuration, Aventail Connect will automatically proxy their allowed application traffic into the private network. In this situation, Aventail Connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server. Then, based on the

security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed")

18. As mention above, Aventail disclosed both DNS request and VPN establish, Aventail did not explicitly detail the VPN. Such detail VPN (e.g., see Figs. 1-3 and 9, pages 6, 9, 11-12, 15, 22-28, etc.) is clearly taught by VPN Overview. Thus, it would have been obvious to one of ordinary skilled in the art to combine the teaching of Aventail with the well-known VPN (e.g., VPN Overview) so that the system with the feature of enhanced security, effectively monitoring and directing network traffic would be archived as suggested by Aventail (e.g., see page 1).

19. As to claims 2-10 and 16-24, those features are well known the art at the time the invention was made.

20. As to claims 13 and 27, Aventail further disclosed the steps of: establishing an IP address hopping scheme between the client and the target (e.g., see page 68 the Aventail MultiProxy feature that allows Aventail Connect to traverse multiple firewalls by making connection through successive proxy serves)

21. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

The references are cited in the Form PTO-892 for the applicant's review.

A shortened statutory period for response to this action is set to expire 3 (three) months and 0 (zero) days from the mail date of this letter.

Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.

If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.

Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).

Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Krisna Lim whose telephone number is 571-272-3956 The examiner can normally be reached on Tuesday to Friday from 7:10 AM to 5:40 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Krista Zele, can be reached on 571-272-7288. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KI
February 25, 2012

/Krisna Lim/
Primary Examiner Art Unit 2453

Notice of References Cited	Application/Control No. 13/336,790	Applicant(s)/Patent Under Reexamination LARSON ET AL.	
	Examiner KRISNA LIM	Art Unit 2453	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,813,777	11-2004	Weinberger et al.	725/76
*	B	US-2009/0199285	08-2009	Agarwal et al.	726/9
*	C	US-2009/0193513	07-2009	Agarwal et al.	726/15
*	D	US-2009/0193498	07-2009	Agarwal et al.	726/1
*	E	US-2008/0144625	06-2008	Wu et al.	370/392
*	F	US-7,584,500	09-2009	Dillon et al.	726/3
*	G	US-7,852,861	12-2010	Wu et al.	370/401
*	H	US-2005/0108517	05-2005	Dillon et al.	713/150
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13336790	LARSON ET AL.
	Examiner	Art Unit
	KRISNA LIM	2453

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	02/25/2012								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								
	24	✓								
	25	✓								
	26	✓								
	27	✓								
	28	✓								

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	63	((VICTOR) near2 (LARSON)).INV.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/02/23 09:27
L2	193	((ROBERT) near2 (SHORT)).INV.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/02/23 09:28
L3	0	((EDMOND) near2 (MUNGER)).INV.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/02/23 09:28
L4	0	((EDMOND) near2 (MUNGER)).INV.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/02/23 09:29
L5	96	((MICHAEL) near2 (WILLIAMSON)).INV.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/02/23 09:29
L6	108552	(secure same communication)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/02/23 09:39
L7	1343	(request same network same address same lookup)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/02/23 09:40
L8	132	l6 and l7	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/02/23 09:40
L9	73	l8 and (VPN or (virtual same private same network))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/02/23 09:40
L10	46	l9 and (domain same name)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/02/23 09:42

2/23/2012 9:55:18 AM

Petitioner Apple Inc. - Exhibit 1002, p. 239

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13336790	LARSON ET AL.
	Examiner	**Art Unit**
	KRISNA LIM	2453

SEARCHED			
Class	**Subclass**	**Date**	**Examiner**
709	223-227	02/23/2012	kl

SEARCH NOTES		
Search Notes	**Date**	**Examiner**
East, Inventors	02/23/2012	kl

INTERFERENCE SEARCH			
Class	**Subclass**	**Date**	**Examiner**

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 6217

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/336,790	12/23/2011	709	2453	77580-151(VRNK-1CP3CNFT1)

APPLICANTS

Victor Larson, Fairfax, VA;
Robert Dunham Short III, Leesburg, VA;
Edmond Colby Munger, Crownsville, MD;
Michael Williamson, South Riding, VA;

**** CONTINUING DATA ***************************

This application is a CON of 13/049,552 03/16/2011
which is a CON of 11/840,560 08/17/2007 PAT 7,921,211
which is a CON of 10/714,849 11/18/2003 PAT 7,418,504
which is a CON of 09/558,210 04/26/2000 ABN
which is a CIP of 09/504,783 02/15/2000 PAT 6,502,135
which is a CIP of 09/429,643 10/29/1999 PAT 7,010,604
which claims benefit of 60/106,261 10/30/1998
and claims benefit of 60/137,704 06/07/1999

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

01/09/2012

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /KRISNA LIM/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		VA	40	28	2

ADDRESS

McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096
UNITED STATES

TITLE

SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

FILING FEE RECEIVED		
2030	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

Best Available Copy

3-26-12 3/26/12

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

OPAP IAP23 MAR 23 2012 PATENT & TRADEMARK OFFICE

CERTIFICATION STATEMENT

[X] Under 37 C.F.R. 1.98(d), copies of all patent, publication, pending U.S. application or other information that was previously submitted to, or cited by the USPTO in an earlier application are not required. Applicant will provide copies of the previously submitted references at the Examiner's request. **Enclosed are copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).**

This application claims priority from and is a continuation of a co-pending U.S. Application No. 13/049,552, filed March 16, 2011, which is a continuation of U.S. Application No. 11/840,560, filed August 17, 2007, now U.S. Patent No. 7,921,211, which is a continuation of U.S. Application No. 10/714,849, filed November 18, 2003, now U.S. Patent No. 7,418,504, which is a continuation of U.S. Application No. 09/558,210, filed April 26, 2000, now abandoned, which is a continuation-in-part of U.S. Application No. 09/504,783, filed on February 15, 2000, now U.S. Patent No. 6,502,135, issued December 31, 2002.

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[ ] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[X] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Date: 3/22/12

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

03/27/2012 HVUONG1 00000012 501133 13336790
01 FC:1806 180.00 DA

DM_US 32511456-1.077580.0151

OPAP
MAR 2 3 2012
IAP23
PATENT & TRADEMARK OFFICE

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

OPAP
MAR 2 3 2012
IAP23
PATENT & TRADEMARK OFFICE

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc Code: TRAN.LET
Document Description: Transmittal Letter

OPAP
MAR 23 2012
PATENT & TRADEMARK OFFICE

PTO/SB/21 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission	52

Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Attorney Docket Number	077580-0151 (VRNK-0001CP3CNFT1)

ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
  - [x] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [x] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [x] Other Enclosure(s) (please Identify below):

Remarks

16 Boxes which include copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	McDermott, Will and Emery		
Signature			
Printed name	Toby H. Kusmer		
Date	March 23, 2012	Reg. No.	26,408

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name		Date	

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

MAR 23 2012
PATENT & TRADEMARK OFFICE

PTO/SB/17 (09-11)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

FEE TRANSMITTAL

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Examiner Name	Krisna Lim
Art Unit	2453
Attorney Docket No.	77580-151 VRNK-0001CP3CNFT1

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 180.00

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☑ Deposit Account Deposit Account Number: 50-1133 Deposit Account Name: McDermott, Will and Emery

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☑ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**

☑ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☐ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

Application Type	FILING FEES Fee ($)	FILING FEES Small Entity Fee ($)	SEARCH FEES Fee ($)	SEARCH FEES Small Entity Fee ($)	EXAMINATION FEES Fee ($)	EXAMINATION FEES Small Entity Fee ($)	Fees Paid ($)
Utility	380	190	620	310	250	125	
Design	250	125	120	60	160	80	
Plant	250	125	380	190	200	100	
Reissue	380	190	620	310	750	375	
Provisional	250	125	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	60	30
Each independent claim over 3 (including Reissues)	250	125
Multiple dependent claims	450	225

Total Claims _____ - 20 or HP = _____ x Extra Claims _____ Fee ($) _____ = Fee Paid ($) _____

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims _____ - 3 or HP = _____ x Extra Claims _____ Fee ($) _____ = Fee Paid ($) _____

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims Fee ($) _____ Fee Paid ($) _____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets _____ - 100 = _____ / 50 = Extra Sheets _____ Number of each additional 50 or fraction thereof _____ (round up to a whole number) x Fee ($) _____ = Fee Paid ($) _____

4. OTHER FEE(S)

	Fees Paid ($)
Non-English Specification, $130 fee (no small entity discount)	
Other (e.g., late filing surcharge): Information Disclosure Statement Filing Fee	$180.00

SUBMITTED BY

Signature		Registration No. (Attorney/Agent) 26,418	Telephone 617-535-4000
Name (Print/Type)	Toby H. Kusmer		Date March 23, 2012

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

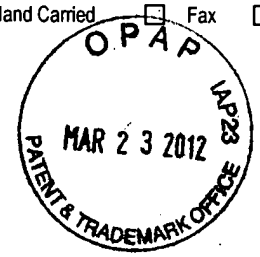
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Applicant: Victor Larson. Docket #. 077580-0151 (VRNK-0001CP3CNFT1

Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES Serial/Reg./Patent No. 13/336,790

Date Sent: March 23, 2012 ☐ Hand Carried ☐ Fax ☐ Electronic ☐ Cert. of Mailing ☒ Express Mail Nos.

EV643771728US
EV643771731US
EV643771743US
EV643771759US
EV643771762US
EV643771776US
EV643771802US
EV643771816US
EV643771780US
EV643771793US



☒ Transmittal Letter

X IDS FORM 1449 (50 pages)

X 16 Boxes of cited references (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).

☒ Fee Transmittal

☐ Response to Missing Parts Notice

☐ Copy of Missing Parts Notice

☐ Replacement Drawing

☐ Maintenance Fee for _____years after grant

☐ Fee Address Indication Form

☐ Terminal Disclaimer

☐ Petition to Commissioner

☐ Status Inquiry

☒ Other RETURN POSTCARD

Check for $	0	☐ Charge Deposit Acct. 50-1133		Atty Init.	THK	Tkpr. #	5470	Secy. or PL:	K. Jones

CMS
Descrip.:

THE PATENT AND TRADEMARK OFFICE DATE STAMPED HEREON IS ACKNOWLEDGEMENT THAT THE ITEMS, CHECKED ABOVE, WERE RECEIVED BY THE PTO ON THE DATE STAMPED.

Accounting

3-26-12 3/26/12 1FW

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

OPAP IAP23 MAR 23 2012 PATENT & TRADEMARK OFFICE

CERTIFICATION STATEMENT

[X] Under 37 C.F.R. 1.98(d), copies of all patent, publication, pending U.S. application or other information that was previously submitted to, or cited by the USPTO in an earlier application are not required. Applicant will provide copies of the previously submitted references at the Examiner's request. **Enclosed are copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).**

This application claims priority from and is a continuation of a co-pending U.S. Application No. 13/049,552, filed March 16, 2011, which is a continuation of U.S. Application No. 11/840,560, filed August 17, 2007, now U.S. Patent No. 7,921,211, which is a continuation of U.S. Application No. 10/714,849, filed November 18, 2003, now U.S. Patent No. 7,418,504, which is a continuation of U.S. Application No. 09/558,210, filed April 26, 2000, now abandoned, which is a continuation-in-part of U.S. Application No. 09/504,783, filed on February 15, 2000, now U.S. Patent No. 6,502,135, issued December 31, 2002.

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[ ] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[X] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Date: 3/22/12

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

03/27/2012 HVUONG1 00000012 501133 13336790
01 FC:1806 180.00 DA

DM_US 32511456-1.077580.0151

OPAP
MAR 23 2012
IAP23
PATENT & TRADEMARK OFFICE

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

OPAP
MAR 2 3 2012
IAP23
PATENT & TRADEMARK OFFICE

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

EFS Code: TRAN.LET
Document Description: Transmittal Letter

PTO
MAR 23 2012
PATENT & TRADEMARK OFFICE

PTO/SB/21 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission	52

Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Attorney Docket Number	077580-0151 (VRNK-0001CP3CNFT1)

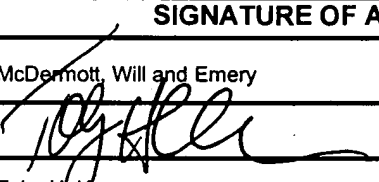
ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
  - [x] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [x] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [x] Other Enclosure(s) (please Identify below):

Remarks

16 Boxes which include copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	McDermott, Will and Emery		
Signature			
Printed name	Toby H. Kusmer		
Date	March 23, 2012	Reg. No.	26,408

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name		Date	

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

MAR 23 2012
PATENT & TRADEMARK OFFICE

PTO/SB/17 (09-11)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

FEE TRANSMITTAL

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Examiner Name	Krisna Lim
Art Unit	2453
Attorney Docket No.	77580-151 VRNK-0001CP3CNFT1

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 180.00

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☑ Deposit Account Deposit Account Number: 50-1133 Deposit Account Name: McDermott, Will and Emery

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☑ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**

☑ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☐ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

Application Type	FILING FEES Fee ($)	FILING FEES Small Entity Fee ($)	SEARCH FEES Fee ($)	SEARCH FEES Small Entity Fee ($)	EXAMINATION FEES Fee ($)	EXAMINATION FEES Small Entity Fee ($)	Fees Paid ($)
Utility	380	190	620	310	250	125	
Design	250	125	120	60	160	80	
Plant	250	125	380	190	200	100	
Reissue	380	190	620	310	750	375	
Provisional	250	125	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	60	30
Each independent claim over 3 (including Reissues)	250	125
Multiple dependent claims	450	225

Total Claims _____ - 20 or HP = _____ x Extra Claims _____ Fee ($) _____ = Fee Paid ($) _____

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims _____ - 3 or HP = _____ x Extra Claims _____ Fee ($) _____ = Fee Paid ($) _____

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims Fee ($) _____ Fee Paid ($) _____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets _____ - 100 = _____ Extra Sheets _____ / 50 = _____ Number of each additional 50 or fraction thereof (round up to a whole number) x Fee ($) _____ = Fee Paid ($) _____

4. OTHER FEE(S)

	Fees Paid ($)
Non-English Specification, $130 fee (no small entity discount)	
Other (e.g., late filing surcharge): Information Disclosure Statement Filing Fee	$180.00

SUBMITTED BY

Signature		Registration No. (Attorney/Agent) 26,418	Telephone 617-535-4000
Name (Print/Type)	Toby H. Kusmer		Date March 23, 2012

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Applicant: Victor Larson. Docket #. 077580-0151 (VRNK-0001CP3CNFT1

Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES Serial/Reg./Patent No. 13/336,790

Date Sent: March 23, 2012 ☐ Hand Carried ☐ Fax ☐ Electronic ☐ Cert. of Mailing ☒ Express Mail Nos.

EV643771728US
EV643771731US
EV643771743US
EV643771759US
EV643771762US
EV643771776US
EV643771802US
EV643771816US
EV643771780US
EV643771793US

☒ Transmittal Letter

X IDS FORM 1449 (50 pages)

X 16 Boxes of cited references (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).

☒ Fee Transmittal

☐ Response to Missing Parts Notice

☐ Copy of Missing Parts Notice

☐ Replacement Drawing

☐ Maintenance Fee for ___ years after grant

☐ Fee Address Indication Form

☐ Terminal Disclaimer

☐ Petition to Commissioner

☐ Status Inquiry

☒ Other RETURN POSTCARD

Check for $	0	☐ Charge Deposit Acct. 50-1133		Atty Init.	THK	Tkpr. #	5470	Secy. or PL:	K. Jones

CMS
Descrip.:

THE PATENT AND TRADEMARK OFFICE DATE STAMPED HEREON IS ACKNOWLEDGEMENT THAT THE ITEMS, CHECKED ABOVE, WERE RECEIVED BY THE PTO ON THE DATE STAMPED.

Accounting

3/26/12 3-26-12 1FW

Subst. for form 1449/RTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

OPAP IAP23 MAR 23 2012 PATENT & TRADEMARK OFFICE

CERTIFICATION STATEMENT

[X] Under 37 C.F.R. 1.98(d), copies of all patent, publication, pending U.S. application or other information that was previously submitted to, or cited by the USPTO in an earlier application are not required. Applicant will provide copies of the previously submitted references at the Examiner's request. **Enclosed are copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).**

This application claims priority from and is a continuation of a co-pending U.S. Application No. 13/049,552, filed March 16, 2011, which is a continuation of U.S. Application No. 11/840,560, filed August 17, 2007, now U.S. Patent No. 7,921,211, which is a continuation of U.S. Application No. 10/714,849, filed November 18, 2003, now U.S. Patent No. 7,418,504, which is a continuation of U.S. Application No. 09/558,210, filed April 26, 2000, now abandoned, which is a continuation-in-part of U.S. Application No. 09/504,783, filed on February 15, 2000, now U.S. Patent No. 6,502,135, issued December 31, 2002.

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[ ] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[X] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

Date: 3/22/12

03/27/2012 HVUONG1 00000012 501133 13336790
01 FC:1806 180.00 DA

DM_US 32511456-1.077580.0151

OPAP
MAR 23 2012
PATENT & TRADEMARK OFFICE
IAP23

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

OPAP
MAR 23 2012
IAP23
PATENT & TRADEMARK OFFICE

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record..
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc Code: TRAN.LET
Document Description: Transmittal Letter

MAR 23 2012
PATENT & TRADEMARK OFFICE

PTO/SB/21 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission	52

Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Attorney Docket Number	077580-0151 (VRNK-0001CP3CNFT1)

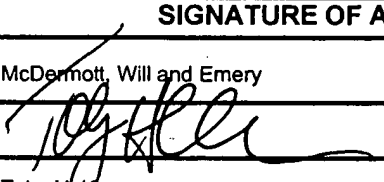
ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
  - [x] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [x] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [x] Other Enclosure(s) (please Identify below):

Remarks

16 Boxes which include copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	McDermott, Will and Emery		
Signature			
Printed name	Toby H. Kusmer		
Date	March 23, 2012	Reg. No.	26,408

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name		Date	

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

MAR 23 2012
IAP23
PATENT & TRADEMARK OFFICE

PTO/SB/17 (09-11)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

FEE TRANSMITTAL

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Examiner Name	Krisna Lim
Art Unit	2453
Attorney Docket No.	77580-151 VRNK-0001CP3CNFT1

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT	($)	180.00

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☑ Deposit Account Deposit Account Number: 50-1133 Deposit Account Name: McDermott, Will and Emery

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☑ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**

☑ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☐ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

Application Type	FILING FEES Fee ($)	FILING FEES Small Entity Fee ($)	SEARCH FEES Fee ($)	SEARCH FEES Small Entity Fee ($)	EXAMINATION FEES Fee ($)	EXAMINATION FEES Small Entity Fee ($)	Fees Paid ($)
Utility	380	190	620	310	250	125	
Design	250	125	120	60	160	80	
Plant	250	125	380	190	200	100	
Reissue	380	190	620	310	750	375	
Provisional	250	125	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	60	30
Each independent claim over 3 (including Reissues)	250	125
Multiple dependent claims	450	225

Total Claims	Extra Claims	Fee ($)	Fee Paid ($)
_____ - 20 or HP =	_____	x _____	= _____

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims	Extra Claims	Fee ($)	Fee Paid ($)
_____ - 3 or HP =	_____	x _____	= _____

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims Fee ($)	Multiple Dependent Claims Fee Paid ($)
_____	_____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof	Fee ($)	Fee Paid ($)
_____ - 100 =	_____ / 50 =	_____ (round up to a whole number)	x _____	= _____

4. OTHER FEE(S)

	Fees Paid ($)
Non-English Specification, $130 fee (no small entity discount)	
Other (e.g., late filing surcharge): Information Disclosure Statement Filing Fee	$180.00

SUBMITTED BY			
Signature		Registration No. (Attorney/Agent) 26,418	Telephone 617-535-4000
Name (Print/Type)	Toby H. Kusmer		Date March 23, 2012

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Applicant: Victor Larson. Docket #. 077580-0151 (VRNK-0001CP3CNFT1

Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES Serial/Reg./Patent No. 13/336,790

Date Sent: March 23, 2012 ☐ Hand Carried ☐ Fax ☐ Electronic ☐ Cert. of Mailing ☒ Express Mail Nos.

EV643771728US
EV643771731US
EV643771743US
EV643771759US
EV643771762US
EV643771776US
EV643771802US
EV643771816US
EV643771780US
EV643771793US

☒ Transmittal Letter

X IDS FORM 1449 (50 pages)

X 16 Boxes of cited references (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).

☒ Fee Transmittal

☐ Response to Missing Parts Notice

☐ Copy of Missing Parts Notice

☐ Replacement Drawing

☐ Maintenance Fee for _____years after grant

☐ Fee Address Indication Form

☐ Terminal Disclaimer

☐ Petition to Commissioner

☐ Status Inquiry

☒ Other RETURN POSTCARD

Check for $	0	☐ Charge Deposit Acct. 50-1133		Atty Init.	THK	Tkpr. #	5470	Secy. or PL:	K. Jones

CMS
Descrip.:

THE PATENT AND TRADEMARK OFFICE DATE STAMPED HEREON IS ACKNOWLEDGEMENT THAT THE ITEMS, CHECKED ABOVE, WERE RECEIVED BY THE PTO ON THE DATE STAMPED.

Accounting

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION International Bureau

B1001

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 11/00 | A1

(11) International Publication Number: WO 00/70458

(43) International Publication Date: 23 November 2000 (23.11.00)

(21) International Application Number: PCT/US00/08219

(22) International Filing Date: 15 May 2000 (15.05.00)

(30) Priority Data:
60/134,547 17 May 1999 (17.05.99) US

(71) Applicant: COMSEC CORPORATION [US/US]; 10217 Cedar Pond Drive, Vienna, VA 22182 (US).

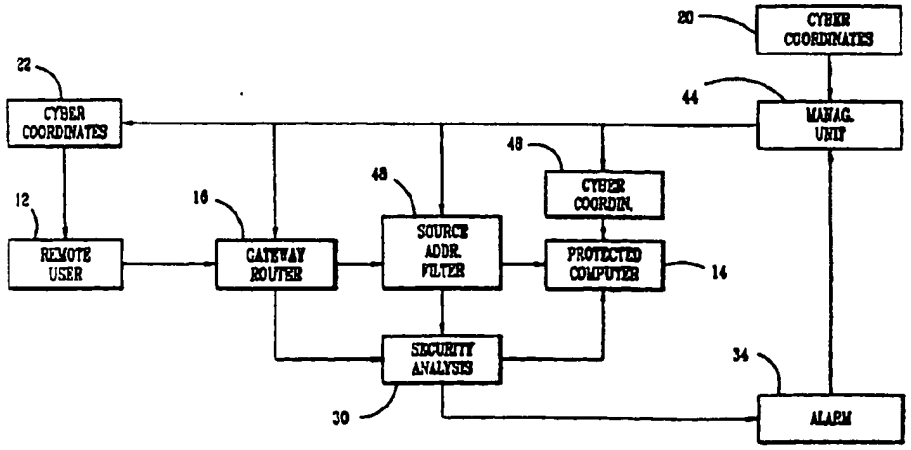
(72) Inventor: SHEYMOV, Victor, I.; 10217 Cedar Pond Drive, Vienna, VA 22182 (US).

(74) Agent: SIXBEY, Daniel, W.; Nixon Peabody LLP, Suite 800, 8180 Greensboro Drive, McLean, VA 22102 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: METHOD OF COMMUNICATIONS AND COMMUNICATION NETWORK INTRUSION PROTECTION METHODS AND INTRUSION ATTEMPT DETECTION SYSTEM



(57) Abstract

The intrusion protection method and system for a communication network provides address agility wherein the cyber coordinates of a target host (14) are changed both on a determined time schedule and when an intrusion attempt is detected. The system includes a managment unit (18) which generates a random sequence of cyber coordinates and maintains a series of tables containing the current and next set of cyber coordinates. These cyber coordinates are distributed to authorized users (12) under an encryption process to prevent unauthorized access.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

METHOD OF COMMUNICATIONS AND COMMUNICATION NETWORK INTRUSION PROTECTION METHODS AND INTRUSION ATTEMPT DETECTION SYSTEM

This application is a continuation-in-part application of U.S. Serial No. 60/134,547 filed May 17, 1999.

Background Art

Historically, every technology begins its evolution focusing mainly on performance parameters, and only at a certain developmental stage does it address the security aspects of its applications. Computer and communications networks follow this pattern in a classic way. For instance, first priorities in development of the Internet were reliability, survivability, optimization of the use of communications channels, and maximization of their speed and capacity. With a notable exception of some government systems, communications security was not an early high priority, if at all. Indeed, with a relatively low number of users at initial stages of Internet development, as well as with their exclusive nature, problems of potential cyber attacks would have been almost unnatural to address, considering the magnitude of other technical and organizational problems to overcome at that time. Furthermore, one of the ideas of the Internet was "democratization" of communications channels and of access to information, which is almost contradictory to the concept of security. Now we are faced with a situation, which requires adequate levels of security in communications while preserving already achieved "democratization" of communications channels and access to information.

All the initial objectives of the original developers of the Internet were achieved with results spectacular enough to almost certainly surpass their expectations. One of the most remarkable results of the Internet development to date is the mentioned "democratization". However in its unguarded way "democratization" apparently is either premature to a certain percentage of the Internet users, or contrary to human nature, or both. The fact remains that this very percentage of users presents a serious threat to the integrity of national critical infrastructure, to privacy of information, and to further advance of commerce by utilization

of the Internet capabilities. At this stage it seems crucial to address security issues but, as usual, it is desirable to be done within already existing structures and technological conventions.

Existing communications protocols, while streamlining communications, still lack underlying entropy sufficient for security purposes. One way to increase entropy, of course, is encryption as illustrated by U.S. Patent No. 5,742,666 to Finley. Here each node in the Internet encrypts the destination address with a code which only the next node can unscramble.

Encryption alone has not proven to be a viable security solution for many communications applications. Even within its core purpose, encryption still retains certain security problems, including distribution and safeguarding of the keys. Besides, encryption represents a "ballast", substantially reducing information processing speed and transfer time. These factors discourage its use in many borderline cases.

Another way is the use of the passwords. This method has been sufficient against humans, but it is clearly not working against computers. Any security success of the password-based security is temporary at best. Rapid advances in computing power make even the most sophisticated password arrangement a short-term solution.

Recent studies clearly indicate that the firewall technology, as illustrated by U.S. Patent No. 5,898,830 to Wesinger et al., also does not provide a sufficient long-term solution to the security problem. While useful to some extent, it cannot alone withstand the modern levels of intrusion cyber attacks.

On the top of everything else, none of the existing security methods, including encryption, provides protection against denial of service attacks. Protection against denial of service attacks has become a critical aspect of communication system security. All existing log-on security systems, including those using encryption, are practically defenseless against such attacks. Given a malicious intent of a potential attacker, it is reasonable to assume that, even having failed with an intrusion attempt, the attacker is still capable of doing harm by disabling the system with a denial of service attack. Since existing systems by definition have to deal with every log-on attempt, legitimate or not, it is certain that these systems cannot defend themselves against a denial of service attack.

The deficiencies of existing security methods for protecting communications systems leads to the conclusion that a new generation of cyber protection technology is needed to achieve acceptable levels of security in network communications.

Summary of the Invention

It is a primary object of the present invention to provide a novel and improved method of communications, and a novel and improved communication network intrusion protection method and systems and novel and improved intrusion attempt detection method and systems, adapted for use with a wide variety of communication networks including Internet based computers, corporate and organizational computer networks (LANs), e-commerce systems, wireless computer communications networks, telephone dial-up systems, wireless dial-up systems, wireless telephone and computer communications systems, cellular and satellite telephone systems, mobile telephone and mobile communications systems, cable based systems and computer databases, as well as protection of network nodes such as routers, switches, gateways, bridges, and frame relays.

Another object of the present invention is to provide a novel and improved communication network intrusion protection method and system which provides address agility combined with a limited allowable number of log-on attempts.

Yet another object of the present invention is to provide a novel and improved intrusion protection method for a wide variety of communication and other devices which may be accessed by a number, address code, and/or access code. This number, address code, and/or access code is periodically changed and the new number, address code, or access code is provided only to authorized users. The new number, address code, or access code may be provided to a computer or a device for the authorized user and not be accessible to others. This identifier causes the user's computer to transmit the otherwise unknown and inaccessible number, address code, and/or access code.

A still further object of the present invention is to provide a novel and improved communication network intrusion protection method and system wherein a plurality of different cyber coordinates must be correctly provided before access is granted to a protected communications unit or a particular piece of information. If all or some cyber coordinates

are not correctly provided, access is denied, an alarm situation is instigated and the affected cyber coordinates may be instantly changed.

For the purposes of this invention cyber coordinates are defined as a set of statements determining location of an object (such as a computer) or a piece of information (such as a computer file) in cyber space. Cyber coordinates include but are not limited to private or public protocol network addresses such as an IP address in the Internet, a computer port number or designator, a computer or database directory, a file name or designator, a telephone number , an access number and/or code, etc.

These and other objects of the present invention are achieved by providing a communication network intrusion protection method and system where a potential intruder must first guess where a target computer such as a host workstation is in cyber space and to predict where the target computer such as a workstation will next be located in cyber space. This is achieved by changing a cyber coordinate (the address) or a plurality of cyber coordinates for the computers such as workstations on a determined or random time schedule and making an unscheduled cyber coordinates change when the system detects an intrusion attempt. A limited number of log-on attempts may be permitted before an intrusion attempt is confirmed and the cyber coordinates are changed. A management unit is provided for generating a random sequence of cyber coordinates and which maintains a series of tables containing current and the next set of addresses. These addresses are distributed to authorized parties, usually with use of an encryption process.

The present invention further provides for a piece of information, a computer or a database intrusion protection method and system where a potential intruder must first guess where a target piece of information such as a computer file or a directory is in cyber space and to predict where the target piece of information will be next in cyber space. This is achieved by changing a cyber coordinate or a plurality of cyber coordinates for the piece of information on a determined or random time schedule and making an unscheduled cyber coordinates change when the system detects an intrusion attempt. A limited number of log-on attempts may be permitted before an intrusion attempt is confirmed and the coordinates changed. A management unit is provided for generating a random sequence of cyber coordinates and which maintains a series of tables containing current and the next set of cyber coordinates. These coordinates are distributed to authorized parties, usually by means

of an encryption process.

The intrusion attempt detection methods and systems are provided to the protected devices and pieces of information as described above by means of categorizing a log-on attempt when all or some of the correct cyber coordinates are not present as an intrusion attempt and by instigating an alarm situation.

Brief Description of the Drawings

Figure 1 is a block diagram of the communication network protection system of the present invention;

Figure 2 is a flow diagram showing the operation of the system of Figure 1;

Figure 3 is a block diagram of a second embodiment of the communication network protection system of the present invention;

Figure 4 is a flow diagram showing the operation of the system of Figure 3;

Figure 5 is a block diagram of a third embodiment of the communication network protection system of the present invention;

Figure 6 is a flow diagram showing the operation of the system of Figure 5; and

Figure 7 is a block diagram of a fourth embodiment of the communication network protection system of the present invention.

Description of the Preferred Embodiments

Existing communications systems use fixed coordinates in cyber space for the communications source and communications receiver. Commonly accepted terminology for the Internet refers to these cyber coordinates as source and destination IP addresses. For

purposes of an unauthorized intrusion into these communication systems, the situation of a cyber attack might be described in military terms as shooting at a stationary target positioned at known coordinates in cyber space. Obviously, a moving target is more secure than the stationary one, and a moving target with coordinates unknown to the intruder is more secure yet. The method of the present invention takes advantage of the cyber space environment and the fact that the correlation between the physical coordinates of computers or other communication devices and their cyber coordinates is insignificant.

While it is difficult to change the physical coordinates of computers or other communications devices, their cyber coordinates (cyber addresses) can be changed much easier, and in accordance with the present invention, may be variable and changing over time. In addition to varying the cyber coordinates over time, the cyber coordinates can immediately be changed when an attempted intrusion is sensed. Furthermore, making the current cyber coordinates available to only authorized parties makes a computer or other communications device a moving target with cyber coordinates unknown to potential attackers. In effect, this method creates a device which perpetually moves in cyber space.

Considering first the method of the present invention as applied to computers and computer networks, the computer's current cyber address may serve also as its initial log-on password with a difference that this initial log-on password is variable. A user, however, has to deal only with a computer's permanent identifier, which is, effectively its assigned "name" within a corresponding network. Any permanent identifier system can be used, and an alphabetic "name" system seems to be reasonably user-friendly. One of such arrangements would call for using a computer's alphabetic Domain Name System, as a cyber address permanent identifier, while subjecting its numeric, or any other cyber address to a periodic change with regular or irregular intervals. This separation will make the security system transparent to the user, who will have to deal only with the alphabetic addresses. In effect, the user's computer would contain an "address book" where the alphabetic addresses are permanent, and the corresponding variable addresses are more complex and periodically updated by a network's management. While a user is working with other members of the network on the name or the alphabetic address basis, the computer conducts communications based on the corresponding variable numeric or other addresses assigned for that particular time.

A variable address system can relatively easily be made to contain virtually any level of entropy, and certainly enough entropy to defy most sophisticated attacks. Obviously, the level of protection is directly related to the level of entropy contained in the variable address system and to the frequency of the cyber address change.

This scenario places a potential attacker in a very difficult situation when he has to find the target before launching an attack. If a restriction on a number of allowable log-on tries is implemented, it becomes more difficult for an attacker to find the target than to actually attack it. This task of locating the target can be made difficult if a network's cyber address system contains sufficient entropy. This difficulty is greatly increased if the security system also limits the number of allowable log-on tries, significantly raising the entropy density.

For the purpose of this invention, entropy density is defined as entropy per one attempt to guess a value of a random variable.

Figure 1 illustrates a simple computer intrusion protection system 10 which operates in accordance with the method of the present invention. Here, a remote user's computer 12 is connected to a protected computer 14 by a gateway router or bridge 16. A management system 18 periodically changes the address for the computer 14 by providing a new address from a cyber address book 20 which stores a plurality of cyber addresses. Each new cyber address is provided by the management system 18 to the router 16 and to a user computer address book 22. The address book 22 contains both the alphabetic destination address for the computer 14 which is available to the user and the variable numeric cyber address which is not available to the user. When the user wants to transmit a packet of information with the alphabetic address for the computer 14, this alphabetic address is automatically substituted for the current numerical cyber address and used in the packet.

With the reference to Figures 1 and 2, when a packet is received by the gateway router or bridge 16 as indicated at 24, the cyber address is checked by the gateway router or bridge at 26, and if the destination address is correct, the packet is passed at 28 to the computer 14. If the destination address is not correct, the packet is directed to a security analysis section 30 which, at 32 determines if the packet is retransmitted with a correct address within a limited number of log-in attempts. If this occurs, the security analysis section transmits the packet to the computer 14 at 28. However, if no correct address is

received within the allowed limited number of log-in attempts, the packet is not transmitted to the computer 14 and the security analysis section activates an alarm section 34 at 36 which in turn causes the management section to immediately operate at 38 to change the cyber address.

Sophisticated cyber attacks often include intrusion through computer ports other than the port intended for a client log-on. If a system principally described in connection with Figures 1 and 2 is implemented, the port vulnerability still represents an opening for an attack from within the network, that is if an attacker has even a low-level authorized access to a particular computer and thus knows its current variable address.

Computer ports can be protected in a way similar to protection of the computer itself. In this case port assignment for the computer becomes variable and is changed periodically in a manner similar to that described in connection with Figures 1 and 2. Then, a current assignment of a particular port is communicated only to appropriate parties and is not known to others. At the same time, similarly to methods described, a computer user would deal with permanent port assignments, which would serve as the ports' permanent "names".

This arrangement in itself may not be sufficient, however, to reliably protect against a port attack using substantial computing power because of a possible insufficient entropy density. Such a protection can be achieved by implementing an internal computer "port router" which would serve essentially the same role for port identifiers as the common gateway router or bridge 16 serves for computer destination addresses.

With reference to Figures 3 and 4 wherein like reference numerals are used for components and operations which are the same as those previously described in connection with Figures 1 and 2, a port router 40 is provided prior to the protected computer 14, and this port router is provided with a port number or designator by the management unit 18. This port number or designator is also provided to the user address book 22 and will be changed when the cyber address is changed, or separately. Thus, with reference to Figure 4, once the cyber address has been cleared at 26, the port number or designator is examined at 42. If the port number is also correct, the data packet will be passed to the computer 14 at 28. If the port number is initially incorrect, the packet is directed to the security analysis section 30 which at 32 determines if the packet is retransmitted with the correct port number within the limited number of log-in attempts.

The port protection feature can be used independently of other features of the system. It can effectively protect nodes of the infrastructure such as routers, gateways, bridges, and frame relays from unauthorized access. This can protect systems from an attacker staging a cyber attack from such nodes.

The method and system of the present invention may be adapted to provide security for both Internet based computer networks and private computer networks such as LANs.

Internet structure allows the creation of an Internet based Private Cyber Network (PCN) among a number of Internet-connected computers. The main concern for using the Internet for this purpose as an alternative to the actual private networks with dedicated communication channels is security of Internet-based networks.

The present invention facilitates establishment of adequate and controllable level of security for the PCNs. Furthermore, this new technology provides means for flexible structure of a PCN, allowing easy and practically instant changes in its membership. Furthermore, it allows preservation of adequate security in an environment where a computer could be a member of multiple PCNs with different security requirements. Utilizing the described concept, a protected computer becomes a "moving target" for the potential intruders where its cyber coordinates are periodically changed and the new coordinates are communicated on a "need to know" basis only to the other members of the PCN authorized to access this computer along with appropriate routers and gateways. This change of cyber coordinates can be performed either by previous arrangement or by communicating future addresses to the authorized members prior to the change. Feasible frequency of such a change can range from a low extreme of a stationary system changing cyber coordinates only upon detection of a cyber attack to an extremely high frequency such as with every packet. The future coordinates can be transmitted either encrypted or unencrypted. Furthermore, each change of position of each PCN member can be made random in terms of both its current cyber coordinates and the time of the coordinates change. These parameters of a protected PCN member's cyber moves are known only to the PCN management, other PCN members with authorization to communicate with this particular member, and appropriate gateways and routers. PCN management would implement and coordinate periodic cyber coordinates changes for all members of the PCN. While the PCN management is the logical party to make all the notification of the cyber coordinates changes, in certain instances it

could be advantageous to shift a part of this task to a PCN member computer itself. With certain limitations, the routers and gateways with the "need to know" the current address of the protected computer are located in cyber space in the general vicinity of the protected computer. In such instances the protected computer could be in a better position to make the mentioned notifications of nearby routers and gateways.

The address changes could be done simultaneously for all the members of the PCN, or separately, particularly if security requirements for the members substantially differ. The latter method is advantageous, for instance, if some of the computers within the PCN are much more likely than others to be targeted by potential intruders. A retail banking PCN could be an example of such an arrangement where the bank's computer is much more likely to be attacked than a customer's computer. It should be noted that, while in certain cases some members of the PCN may not require any protection at all, it still is prudent to provide it as long as the computer belongs to a protected PCN. The correct "signature" of the current "return address" would serve as additional authenticity verification. In the above example of the retail banking, while many customers' computers may not require any protection, assigning variable addresses to them would serve as an additional assurance to the bank that every log-on is authorized. In fact, this system automatically provides two-tier security. In order to reach a protected computer, the client computer has to know the server computer current cyber address in the first place. Then, even if a potential intruder against odds "hits" the correct current address the information packet is screened for the correct "signature" or return address. If that signature does not belong to the list of the PCN's current addresses, the packet is rejected. In high security instances this should trigger an unscheduled address change of the protected computer.

With the reference to Figures 5 and 6 which illustrate this two-tier security system, a network management unit 44 provides different unique cyber coordinates to the address books for each computer in the system (two computers 12 and 14 with address books 22 and 46 respectively being shown). Now when the computer 12 sends a data packet to the computer 14, the gateway router or bridge 16, first checks for the correct current destination address for the computer 14 at 26 in the manner previously described. If the destination address is correct, a source address sensor 48 checks at 50 to determine if the correct source address (i.e. return address) for the computer 12 is also present. If both correct addresses are

present, the datu packet is passed to the computer 14 at 28, but if the correct source address is not present, the data packet is passed to the security analysis section 30 where at 32 where it is determined if a correct source address is received within the acceptable number of log-on tries. If the correct return address is not received, an alarm situation is activated at 36 and the network management system operates at 38 to change the cyber address of the computer 14

In addition to the penetration (hacking) detection and protection, the system above provides real-time detection of a cyber attack and protection against "flooding" denial of service attacks. A gateway router or bridge 16 filters all the incorrectly addressed packets thus protecting against "flooding". Further yet, since the "address book" of the protected network contains only trusted destinations, this system also protects against instructive viruses or worms if such are present or introduced into the network. For the purpose of this invention, an instructive virus or worm is defined as a foreign unit of software introduced into a computer system so it sends certain computer data to otherwise unauthorized parties outside of the system.

Elements of the system described above are: a gateway router or bridge 16, a computer protection unit, and a management unit. A gateway router or bridge represents an element of collective defense for the network, while the source address filter and the "port router" and filter represent a unit of individual defense for a member computer. This individual defense unit (server unit) can be implemented either as a standalone computer, as a card in the protected computer, as software in the protected computer, or imbedded into the protected computer operating system. For further improvement of the overall security, port assignments can be generated autonomously from the management unit thus creating a "two keys" system in a cryptographic sense. This would allow for security to still be in place even if a security breach happened at the security management level.

The method and system of the present invention minimize human involvement in the system. The system can be configured in such a way that computer users deal only with simple identifiers or names permanently assigned to every computer in the network. All the real (current) cyber coordinates can be stored separately and be inaccessible to the user, and could be available to the appropriate computers only. This approach both enhances security and makes this security system transparent to the user. The user deals only with the simple

alphabetic side of the "address book", and is not bothered with the inner workings of the security system. A telephone equivalent of this configuration is an electronic white pages residing in a computerized telephone set, which is automatically updated by the telephone company. The user just has to find a name, and push the "connect" button while the telephone set does the rest of the task.

A numeric cyber address system, based on the Internet host number could be relatively easily utilized for the discussed security purposes, however a limitation exists for this address system in its current form represented by the IPv.4 protocol. This limitation is posed by the fact that the address is represented by a 32-bit number. 32-bit format does not contain sufficient entropy in the address system to enable establishment of adequate security. This is a particularly serious limitation in regard to securing an entire network. The availability of the network numbers are limited to the extent that not only entropy, but a simple permanently assigned number is becoming more and more difficult to obtain with the rapid expansion of the Internet.

If this address system is to be used for the security purposes, than the format of the host number should be adequately expanded to create sufficient size of the address numbers field in the system. If this is done, than the corresponding address in the Domain Name System (DNS) could be conveniently used as permanent identifier for a particular computer and the Internet host number would be variable, creating a moving regime of a protected computer. Currently being implemented IPv.6 (IPNG) protocol solves this problem by providing sufficient entropy.

Another way to achieve the same goal is to use the DNS address as a variable for security purposes. This way, the traditional Internet DNS address system would not be affected and no change in format is required. The relevant part of the protected computer's DNS address would become a variable, utilizing more characters than the alphabet, with a very large number of variations, also creating sufficient level of entropy.

Yet another way to implement the same method is to utilize the geographic zone-based system. While its utilization is somewhat similar to the DNS system, it offers some practical advantages for security use. Naturally, when a computer is protected by a security system, it is still essential to preserve the communication redundancy of the Internet communications. However, the redundancy may suffer if only a limited number of the

routers and gateways are informed of the protected computer current cyber address. This effect could be particularly important with the members of a particular protected network vastly remote in geographic terms. The necessary notification of a large number of the routers and gateways can also become problematic, not only technically, but also because it can decrease the level of security. In this sense a geographic zone-based system offers advantages since the variable part of the computer's cyber address could be made to involve only certain geographic locale while initial routing of the information packet could be done by the traditional method. After the packet has been moved to the general vicinity of the addressee computer, it would get into the area of the "informed" routers and gateways. This scheme would simplify the notification process of the routers as well as improve security by limiting the number of the "need to know" parties. It is important to recognize that, after the "general" part of the cyber address caused the information packet to arrive in a cyber vicinity of the addressee, virtually any, even private, address system can be used for the rest of he the delivery. This would further increase the level of underlying entropy in the system.

While certain specific address systems have been discussed, it is an important quality of the present invention that it can be implemented with virtually any address system.

Corporate and organizational computer networks such as LANs or, at least those in closed configurations, do not possess as much vulnerability to cyber attacks as Internet-based networks. However, even in these cases, their remote access security is a subject of concern. This is especially visible when a private network (PN) contains information of different levels of confidentiality with access restricted to appropriate parties. In other words, along with other generally accessible organizational information, an organizational PN can contain information restricted to certain limited groups. Enforcement of these restrictions requires a remote access security system. Usually these security systems employ a password-based scheme of one type or another and, perhaps, a firewall. However, reliance on passwords may not be entirely justified since the passwords can be lost or stolen, giving a malicious insider with a low access level a reasonable chance of access to information intended only for higher levels of access. Furthermore, in some cases use of cracking techniques from such a position is not entirely out of the question. Such an occurrence can relatively easily defeat both the password and the firewall. This would prevent a LAN from a cyber attack launched from within the network.

The present invention provides adequate security to such PCNs without reliance on the passwords and to limit access to only appropriate computers. Then, the task of overall information access security practically would be narrowed down to control of physical access to a particular computer, usually a less complicated feat.

Similarly to the systems described for Internet-based networks, a "closed" LAN as well as an Internet-based LAN can be protected by implementation of periodic changes of the members' network addresses and communicating those changes to the appropriate parties. This way, the lowest access level computers would have the lowest rate of address change. The rate of the address change would increase with the level of access. This system would ensure that all the PCN computers with legitimate access to a particular computer within the PCN would be informed of its location. Furthermore, it will ensure that the current location of a computer with restricted information would be unknown to the parties without the legitimate access clearance. For instance, a superior's computer would be able to access his subordinate's computer but not vice versa.

Also similarly to the systems described for the PCNs, a PCN computer would contain an "address book" where the user can see and use only the permanent side of it with identifiers of all computers accessible to him while the actual communication functions are performed by the computer using the variable side of the "address book" periodically updated by the PN management. To further enhance security, in addition to the computer address system management, the PCN Administrator can implement an automatic security monitoring system where all wrongly addressed log-on attempts would be registered and analyzed for security purposes.

Thus the method and system of the present invention would allow reliable protection against unauthorized remote access to information from within a PN while providing a great deal of flexibility, where the granted access can be revised easily and quickly.

A greatly enhanced intrusion protection system and method can be achieved by combining the operating systems of Figures 1-6. Now an arriving data packet would first be screened by a gateway router or a similar device for a correct destination address. If the destination address is correct, the packet is passed for further processing. If the destination address is incorrect, the alarm is triggered and the packet is passed to the network security managing unit for security analysis.

The packet with correct destination address is then screened for a correct source address. If the source address is correct, the packet is passed to the receiver computer. If the source address is incorrect, the alarm is triggered and the packet is passed to the network security managing unit for security analysis.

Then, the packet with a correct destination address and a correct source address is screened for a correct allowed port coordinate such as port number. If the port coordinate is correct, the packet is passed for further processing. If the port coordinate is incorrect, the alarm is triggered and the packet is passed to the network security managing unit for security analysis.

Finally, the packet with a correct destination and source addresses and a correct port designator is screened for data integrity by application of authentication check such as a checksum. If the authentication check is passed, the packet is passed to the addressee computer. If the authentication check is failed, the alarm is triggered and the packet is passed to the network security managing unit for security analysis.

The security managing unit analyses all the alarms and makes decisions on necessary unscheduled changes of addresses for appropriate network servers. Also, it can notify law enforcement and pass appropriate data on to it.

Figure 7 illustrates an enhanced computer intrusion protection system indicated generally at 52 for one or more network computers 54. A gateway router or a bridge 58 includes a destination address filter 60 which receives data packets which pass in through a load distribution switch 62. A non-interrogatable network address book 64 stores current network server addresses for the destination address filter 60, and the destination address filter checks each data packet to determine if a legitimate destination address is present.

Packets with legitimate destination addresses are forwarded to a source address filter 66, while packets with illegitimate destination addresses are sent to a security analysis section 68 in a management unit 70.

When a preset traffic load level is reached indicating that an attempt at flooding is being made, the destination address filter causes the load distribution switch 62 to distribute traffic to one or more parallel gateway routers or bridges which collectively forward legitimate traffic and dump the flooding traffic. An alternative arrangement would call for the load distribution function to be done irrespective of the load, utilizing all the parallel

gateways all the time. A source address table 74 stores accessible server's designators and corresponding current addresses for all system servers which may legitimately have access to the computer or computers 54. These addresses are accessed by the source address filter which determines whether or not an incoming data packet with the proper destination address originates from a source with a legitimate source address entered in the source address table 74. If the source address is determined to be legitimate, the data packet is passed to a port address filter 76. Data packets with an illegitimate source address are directed to the security analysis section 68. Alternatively, source address screening can be done at the gateway router or bridge 58 first prior to port filter 76.

A port protection table 78 includes the current port assignments for the computer or computers 54, and these port assignments are accessed by the port designator filter 76 which then determines if an incoming data packet contains legitimate port designation. If it does, it is passed to an actual address translator 80 which forwards the data packet to the specific computer or computers 54 which are to receive the packet. If an illegitimate port address is found by the port address filter 76, the data packet is transmitted to the security analysis section 68.

The management unit 70 is under the control of a security administrator 82. A network membership master file 84 stores a master list of legitimate server's designators along with respective authorized access lists and corresponding current cyber coordinates. The security administrator can update the master list by adding or removing authorized access for every protected computer. An access authorization unit 86 distributes the upgraded relevant portions of the master lists to the address books of the respective authorized servers.

A random character generator 88 generates random characters for use in forming current port designators, and provides these characters to a port designator forming block 90. This port designator forming block forms the next set of network current port designators in conjunction with the master list and these are incorporated for transmission by a port table block 92. Alternatively, port designators can be formed in the computer unit instead of the management unit.

Similarly, a random character generator 94 generates random characters for use in forming current server addresses, and provides these characters to a server address forming

block 96. This server address forming block forms the next set of current network server addresses, and an address table 98 assigns addresses to servers designated on the master list.

A coordinator/dispatcher block 100 coordinates scheduled move of network servers to their next current addresses, provides the next set of network addresses for appropriate servers and routers and coordinates unscheduled changes of addresses on command from the security analysis unit 68. The coordinator/dispatcher block 100 may be connected to an encode/decode block 102 which decodes received address book upgrades from input 104 and encodes new port and server destination addresses to be sent to authorized servers in the system over output 106. Where encoding of new cyber coordinates is used, each authorized computer in the network will have a similar encoding/decoding unit.

The security analysis unit 68 analyses received illegitimate data packets and detects attack attempts. If needed, the security analysis unit orders the coordinator/dispatcher block 100 to provide an unscheduled address change and diverts the attack data packets to an investigation unit 108. This investigation unit simulates the target server keeping a dialog alive with the attacker to permit security personnel to engage and follow the progress of the attacker while tracing the origin of the attack.

Providing security against intrusion for e-commerce systems presents a unique problem, for an important peculiarity of an e-commerce system is that its address must be publicly known. This aspect represents a contradiction to the requirement of the address being known to authorized parties only. However, the only information intended for the general public usually relates to a company catalog and similar material. The rest of the information on a merchant's network is usually considered private and thus should be protected. Using this distinction, a merchant's e-commerce site should be split into two parts: public and private. The public part is set up on a public "catalog" server with a fixed IP address and should contain only information intended for the general public. The rest of the corporate information should be placed in a separate network and protected as described in relation to Figures 1-7.

When a customer has completed shopping and made purchasing decisions concerning the terms and price of the sale, pertinent for the transaction, information is placed in a separate register. This register is periodically swept by a server handling financial transactions ("financial" server), which belongs to the protected corporate network. In fact,

the "catalog" server does not know the current address of the financial transactions server. Thus, even if an intruder penetrates the "catalog" server, the damage is limited to the contents of the catalog and the intruder cannot get an entry to the protected corporate network.

The financial server, having received pending transaction data, contacts the customer, offering a short-term temporary access for finalizing the transaction. In other words, the customer is allowed access just long enough to communicate pertinent financial data such as a credit card number and to receive a transaction confirmation at which point the session is terminated, the customer is diverted back to the catalog server and the financial server is moved to a new cyber address thus making obtained knowledge of its location during the transaction obsolete.

Dial-up communications systems, in respect to their infrastructure channels susceptibility to transmission intercept by unrelated parties, can be separated into two broad categories: easily interceptable, such as cellular and satellite telephone systems and relatively protected such as conventional land-line based telephone systems. Relatively protected systems such as conventional land-line based telephone systems can be protected in the following way. Phone numbers, assigned by a telephone company to a dial-up telephone-based private network serve as the members' computer addresses. As described previously, such a private network can be protected from unauthorized remote access by implementing periodic changes in the addresses, i.e. telephone numbers assigned to the members for transmission by the network along with other designators such as access codes and communicating the changed numbers to the appropriate parties.

For the conventional land-line dial-up telephone systems, while the "last mile" connection remains constant, the assigned telephone number is periodically changed, making the corresponding computer a moving target for a potential attacker. In this case the telephone company serves as the security system manager. It assigns the current variable telephone numbers to the members of a protected, private network, performs notification of all the appropriate parties, and changes the members' current numbers to a new set at an appropriate time. The telephone company switches naturally serve in the role of routers, and thus they can be programmed to perform surveillance of the system, to detect potential intrusion attacks and to issue appropriate alarms.

Periodically changing the current assigned numbers creates system entropy for a potential intruder, making unauthorized access difficult. Obviously, the implementation of this security system is dependent on availability of sufficient vacant numbers at a particular facility of the telephone company. Furthermore, for a variety of practical reasons it is advisable to keep a just vacated number unassigned for a certain period of time. All this may require additional number capacity at the telephone company facility in order to enable it to provide remote access security to a larger number of personal networks while preserving a comfortable level of system entropy.

If the mentioned additional capacity is not available, or a still higher level of entropy is desired, it could be artificially increased by adding an access code to the assigned number. This would amount to adding virtual capacity to the system, and would make a combination of the phone number and access code an equivalent of a computer's telephone address. In effect, this would make a dialed number larger than the conventional format. This method makes a virtual number capacity practically unlimited and, since the process is handled by computers without human involvement, it should not put any additional burden on a user. With or without a virtual number capacity, utilization of this method allows the intrusion attempts to be easily identified by their wrong number and/or code. At the same time, implementation of this system might require some changes in dialing protocols as well as additional capabilities of the telephone switching equipment.

Entropy density can be increased by limiting the number of allowable connection attempts. Similarly to the method described previously, telephone company switching equipment can be made to perform a role of an outside security barrier for the private network. In this case wrongly addressed connection attempts should be analyzed in order to detect possible "sweeping". If such an attempt is detected, tracing the origin of the attempt and notifying the appropriate phone company should not present a problem even with the existing technology.

The simplest form of private network protection under the proposed method and system is when at a predetermined time all the members of a particular network are switched to the new "telephone book" of the network. However, in some cases required level of security for some members of the same private network could substantially differ, or they may face different levels of security risk. In such cases frequency of the phone number

change could be set individually with appropriate notification of the other members of the network. This differentiation enables the telephone company to offer differentiated levels of security protection to its customers even within the same private network.

A telephone company can also offer its customers protected voice private networks which would provide a higher level of privacy protection than the presently used "unlisted numbers." In this configuration the customers' telephone sets are equipped with a computerized dialing device with remotely upgradeable memory which would allow each member of a protected voice network to contain the network "telephone book" and that book is periodically updated by the telephone company.

The telephone company would periodically change the assigned telephone numbers of a protected network to a new set of current numbers. These new numbers would be communicated to the members of a protected voice network through updating their computerized dialing devices.

As a derivative of the described system, an updateable electronic telephone directory system can be also implemented. In this case a customer's phone set would include a computerized dialing device with electronic memory containing a conventional telephone directory and a personal directory as well. This telephone directory can be periodically updated on-line by the telephone company.

Easily interceptable systems such as cellular and satellite telephone systems, in addition to the protection described above, can be protected from "cloning" when their signals can be intercepted and the "identity" of the phone can be cloned for gaining unauthorized access and use of the system by unauthorized parties.

Mobile telephone and mobile communications systems are protected in a manner similar to networks or land based telephone systems. In this instance, the novel and improved method of changing cyber coordinates is designed to reliably protect mobile phone systems from unauthorized use commonly known as cloning as well as to make intercept of wireless communications more difficult than it is at present. With this system the static wireless phone number or other similar identifier is not used for identification and authorization. Instead, a set of private identifiers is generated known only to the phone company and base stations controlling mobile phone calls and used to continually update the mobile phone and base station directories with current valid identifiers. This approach provides vastly superior

protection over current methods requiring that each call be intercepted in order to track and keep current with changing identifiers. Immediate detection of unauthorized attempts to use a cloned phone is realized and law enforcement may be notified in near real time for appropriate action.

Other electronic devices using wireless communications can be protected by the methods and systems described above.

Finally, computers often contain databases with a variety of information. That information in a database often has wide-ranging levels of sensitivity or commercial value. This creates a situation when large computers serve multiple users with vastly different levels of access. Furthermore, even within the same level of access, security considerations require compartmentalization of information when each user has to have access to only a small portion of the database.

The existing systems try to solve this situation by utilizing passwords and internal firewalls. As it was mentioned earlier, password-based systems and firewalls are not sufficient against computerized attacks. In practical terms it means that a legitimate user with a low level of access, utilizing hacking techniques from his station, potentially can break into even the most restricted areas of the database.

This problem can be solved by using the method of the present invention. A piece of information such as a file or a directory in a computer exists in cyber space. Accordingly, it has its cyber address, usually expressed as a directory and/or a file name which defines its position in a particular computer file system. This, in effect, represents the cyber coordinates of that piece of information within a computer.

As described earlier, information security can be provided if a system manager periodically changes the directories and/or file names in the system, i.e. the cyber addresses of the information, and notifies only appropriate parties of the current file names. This method would ensure that each user computer knows locations of only files to which it has legitimate access. Furthermore, a user would not even know of existence of the files to which he has no access.

To further strengthen the system and make it user-friendly, the user would have a personal directory similar to an address book, where only permanent directory and/or file names are accessible to him, while the variable side of the "address book" would be

accessible only to the system manager and upgraded periodically. In this arrangement variable directory and/or file names can contain any required level of entropy, further increasing resistance to attacks from within the system. Additionally, an internal "router" or "filter" can also perform information security monitoring functions, detect intrusion attempts and issue appropriate alarms in real time.

Obviously, in order to ensure information security in such arrangement any computer-wide search by keywords or subject should be disabled and substituted with a search within specific clients' "address books".

The systems and methods described above allow for creation of a feasible infrastructure protection system such as a national or international infrastructure protection system. When detected at specific points cyber attacks are referred to such a system for further analysis and a possible action by law enforcement authorities.

I claim:

1. A method for protecting a communications device which is connected to a communications system against an unauthorized intrusion which includes:

providing the communications device with at least one identifier,

providing the at least one identifier for use in accessing the communications device to entities authorized to access said communications device,

sensing the presence or absence of said identifier before granting access to said communications device,

providing access to said communications device when the use of said at least one correct identifier is sensed

denying access to said communications device and providing said communications device with at least one new identifier when the absence of the correct at least one identifier is sensed during an attempt to access said communications device, and providing said at least one new identifier to entities authorized to access said communications device.

2. The method of claim 1 which includes periodically changing the at least one identifier and providing the changed at least one identifier to the entities authorized to access said communications device.

3. The method of claim 1 which includes providing said communications device with a plurality of separate identifiers,

sensing the presence or absence of all of said plurality of identifiers before granting access to said communications device,

providing access to said communications device when the use of all of said identifiers is sensed, and

denying access to said communications device and providing said communications device with a new plurality of identifiers to replace the previous plurality of identifiers when the absence of any one of the correct identifiers is sensed.

4. The method of claim 3 which includes periodically changing said plurality of

separate identifiers and providing the changed identifiers to the entities authorized to access said communications device.

5. The method of claim 1 which includes permitting a predetermined number of attempts to access said communications device with a correct at least one identifier after the absence of the correct at least one identifier is sensed before providing said communications device with at least one new identifier,

and providing access to said communications device if the correct at least one identifier is sensed during the predetermined number of attempts to access.

6. The method of claim 2 wherein said communications system is a telephone system and said communications device is a telephone.

7. The method of claim 1 wherein said communications system is a computer network with said entities authorized to access said communications device being authorized computers having access to said computer network, said communications device including at least one host computer having access to said computer network.

8. The method of claim 7 which includes periodically changing the at least one identifier for the host computer and providing the changed at least one identifier to the authorized computers.

9. The method of claim 7 which includes providing the authorized computers with an unchangeable, accessible address for the host computer which is used by the authorized computer to activate and transmit the at least one identifier for the host computer when the authorized computer initiates access to the host computer.

10. The method of claim 8 which includes providing each authorized computer with an authorized computer identifier,

providing the host computer with a destination identifier,

causing each authorized computer to access said host computer with at least a host

computer destination identifier and the authorized computer identifier,

sensing the presence or absence of both said host computer destination identifier and an authorized computer identifier before granting access to said host computer,

providing access to said host computer when the use of both a correct host computer destination identifier and an authorized computer identifier is sensed, and

denying access to said host computer and providing said host computer with a new host computer destination identifier when the absence of either a correct host computer destination identifier or a correct authorized computer identifier is sensed.

11. The method of claim 10 which includes permitting a predetermined number of attempts to access said host computer with both a correct host computer destination identifier and an authorized computer identifier after the absence of a correct host computer destination identifier or an authorized computer identifier is sensed before providing said host computer with a new host computer destination identifier, and

providing access to said host computer if correct host computer destination and authorized computer identifier are sensed during the predetermined number of attempts to access the host computer.

12. The method of claim 11 which includes storing said host computer destination identifier as an inaccessible identifier in said authorized computers, and providing said authorized computers with an unchangeable, accessible host computer address, which will activate and transmit the host computer destination identifier when an authorized computer initiates access to the host computer.

13. The method of claim 8 which includes providing said host computer with a host computer destination identifier and a host computer port identifier,

causing each authorized computer to access said host computer with at least the host computer destination identifier and the host computer port identifier,

sensing the presence or absence of both said host computer destination identifier and said host computer port identifier before granting access to said host computer,

providing access to said host computer when the use of both a correct host computer

destination identifier and a correct host computer port identifier are sensed, and

denying access to said host computer and providing said host computer with a new destination identifier and port identifier when the absence of either or both of a correct host computer destination or port identifier is sensed.

14. The method of claim 13 which includes permitting a predetermined number of attempts to access said host computer with both a correct host computer destination and port identifier when either or both an incorrect host computer destination or port identifier is sensed before providing said host computer with a new destination and port identifier, and

providing access to said host computer if both correct host computer destination and port identifiers are sensed during the predetermined number of attempts to access said host computer.

15. The method of claim 14 which includes storing said host computer destination and port identifiers as inaccessible identifiers in said authorized computers and providing said authorized computers with an unchangeable, accessible host computer address which will activate and transmit the host computer destination and port identifiers when an authorized computer initiates access to said host computer.

16. An intrusion protection method for protecting a host computer connected to a computer communications system which includes one or more authorized computers having access to said computer communications system which are authorized to access said host computer which includes:

providing each authorized computer with an authorized computer identifying address,

providing said host computer with a host computer destination identifier and a host computer port identifier,

providing said host computer destination identifier and said host computer port identifier to said authorized computers,

causing each authorized computer to access said host computer with the host computer destination and port identifiers and said authorized computer identifying address,

sensing the presence or absence of said host computer destination and port identifiers

and said authorized computer identifying address before granting access to said host computer,

providing access to said host computer when the use of correct computer destination and port identifiers and a correct authorized computer identifying address is sensed, and

denying immediate access to said host computer when the absence of any one or more of the correct host computer destination and port identifiers or the authorized computer identifying address is sensed.

17. The method of claim 16 which includes periodically changing the host computer destination and port identifiers and providing these changes to the authorized computers.

18. The method of claim 17 which includes storing said host computer destination and port identifiers as inaccessible identifiers in said authorized computer and providing said authorized computers with an unchangeable, accessible host computer address which will activate and transmit the host computer destination and port identifiers when an authorized computer initiates access to said host computer.

19. The method of claim 16 which includes changing the host computer destination and port identifiers when access is denied to said host computer after at least one access attempt has been made and providing these changed identifiers to the authorized computers.

20. The method of claim 16 which includes permitting a predetermined number of attempts to access said host computer with correct host computer destination and port identifiers and a correct authorized computer identifying address after the absence of at least a correct one of said identifiers and authorized computer identifying address is sensed by the host computer and

providing access to said host computer if correct host computer destination and port identifiers and a correct authorized computer identifying address are sensed during the predetermined number of attempts to access said host computer.

21. The method of claim 19 which includes storing said host computer destination and port identifiers as inaccessible identifiers in said authorized computer and providing said authorized computers with an unchangeable, accessible host computer address which will activate and cause transmission of the host computer destination and port identifiers when an authorized computer initiates access to said host computer.

22. The method of claim 20 which includes changing the host computer destination and port identifiers when access is denied to said host computer after at least one access attempt has been made and providing these changed identifiers to the authorized computers.

23. The method of claim 22 which includes storing said host computer destination and port identifiers as inaccessible identifiers in said authorized computer and providing said authorized computers with an unchangeable, accessible host computer address which will activate and cause transmission of the host computer destination and port identifiers when an authorized computer initiates access to said host computer.

24. A method of communication with a remote entity over a communication system which includes

providing the remote entity with at least one remote entity cyber coordinate identifier,

providing the remote entity cyber coordinate identifier to one or more base entities authorized to communicate with said remote entity,

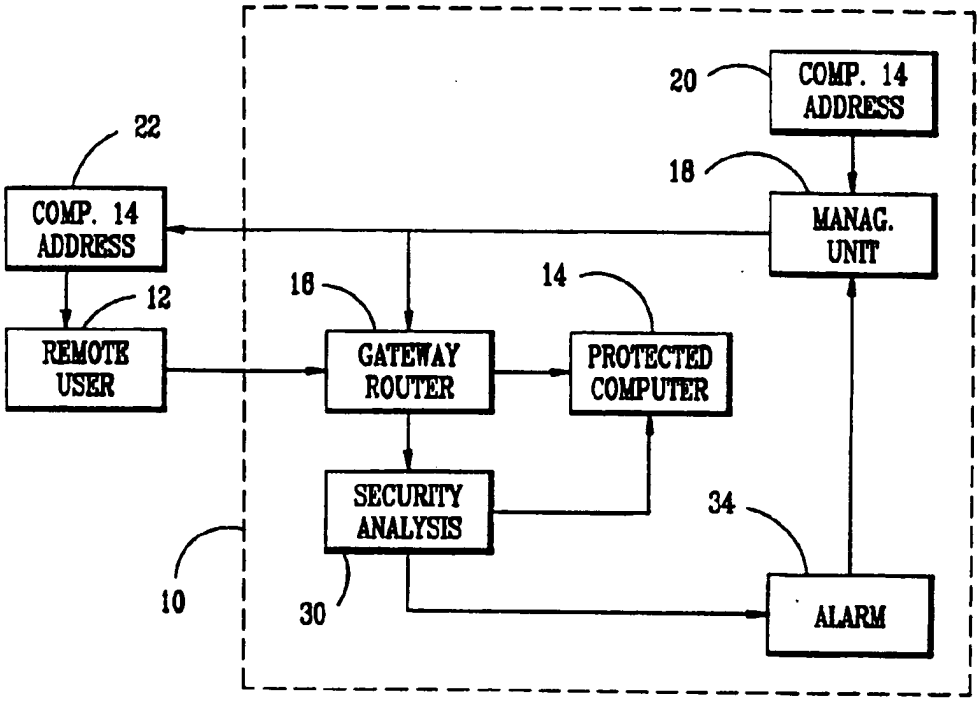
periodically changing the remote entity cyber coordinate identifier to a new remote entity cyber coordinate identifier and

providing the new remote entity cyber coordinate identifier to said one or more base entities.

25. The method of claim 24 which includes changing the remote entity cyber coordinate identifier to a new cyber coordinate identifier in response to an attempt to communicate with said remote entity with an incorrect remote entity cyber coordinate identifier and

providing the new remote entity cyber coordinate identifier to said one or more base entities.

FIG. 1



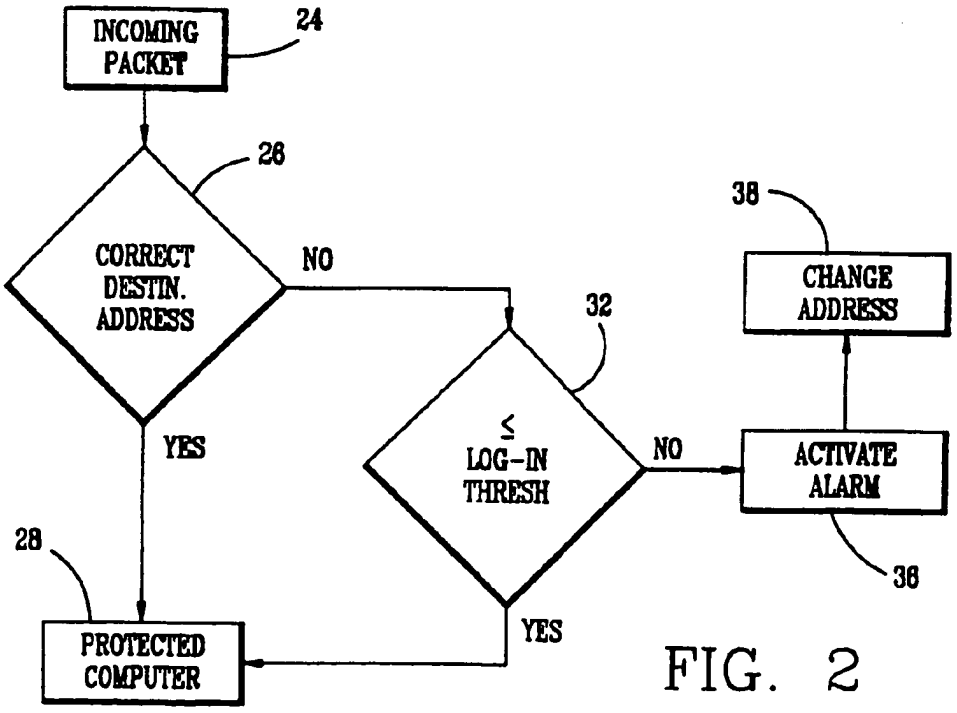


FIG. 2

Petitioner Apple Inc. - Exhibit 1002, p. 291

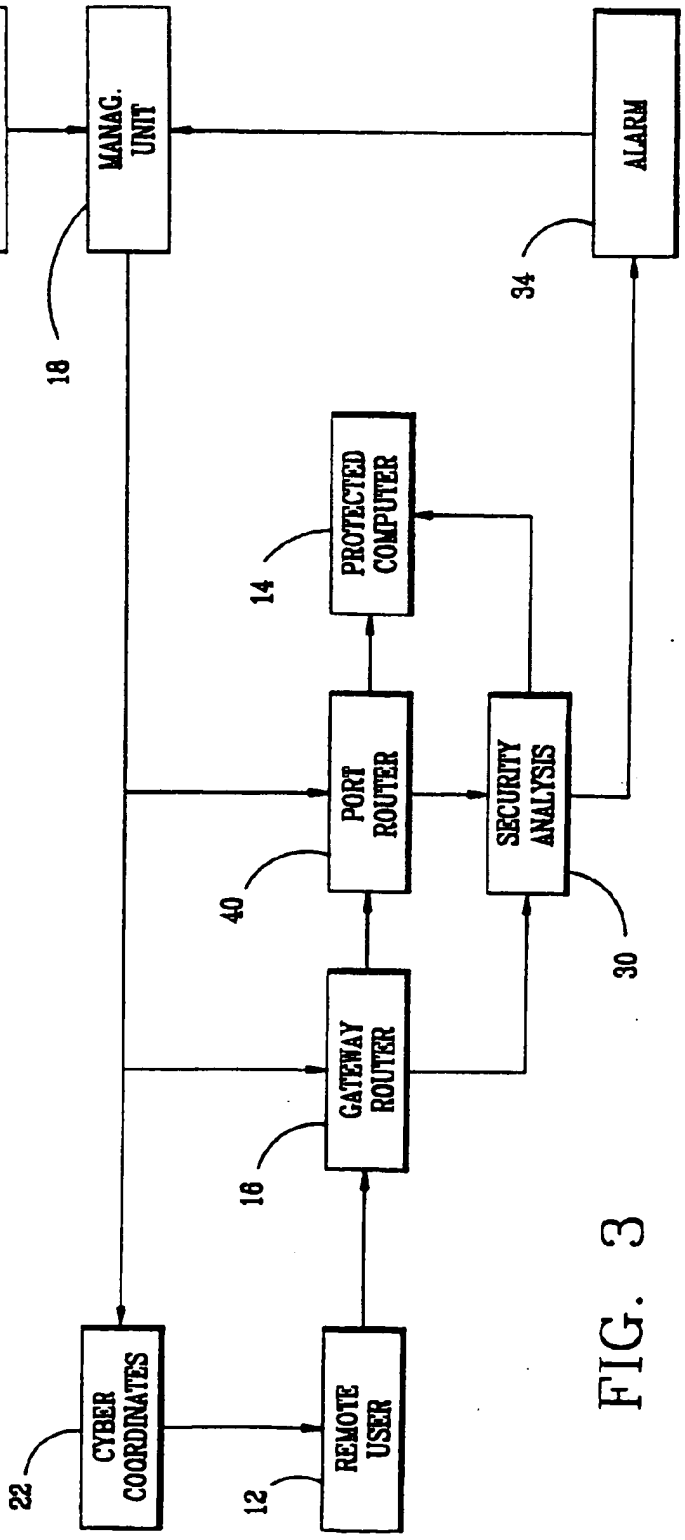

CYBER COORDINATES
MANAG. UNIT
ALARM
20
18
34
PROTECTED COMPUTER
14
PORT ROUTER
SECURITY ANALYSIS
40
30
GATEWAY ROUTER
16
CYBER COORDINATES
REMOTE USER
22
12

FIG. 3

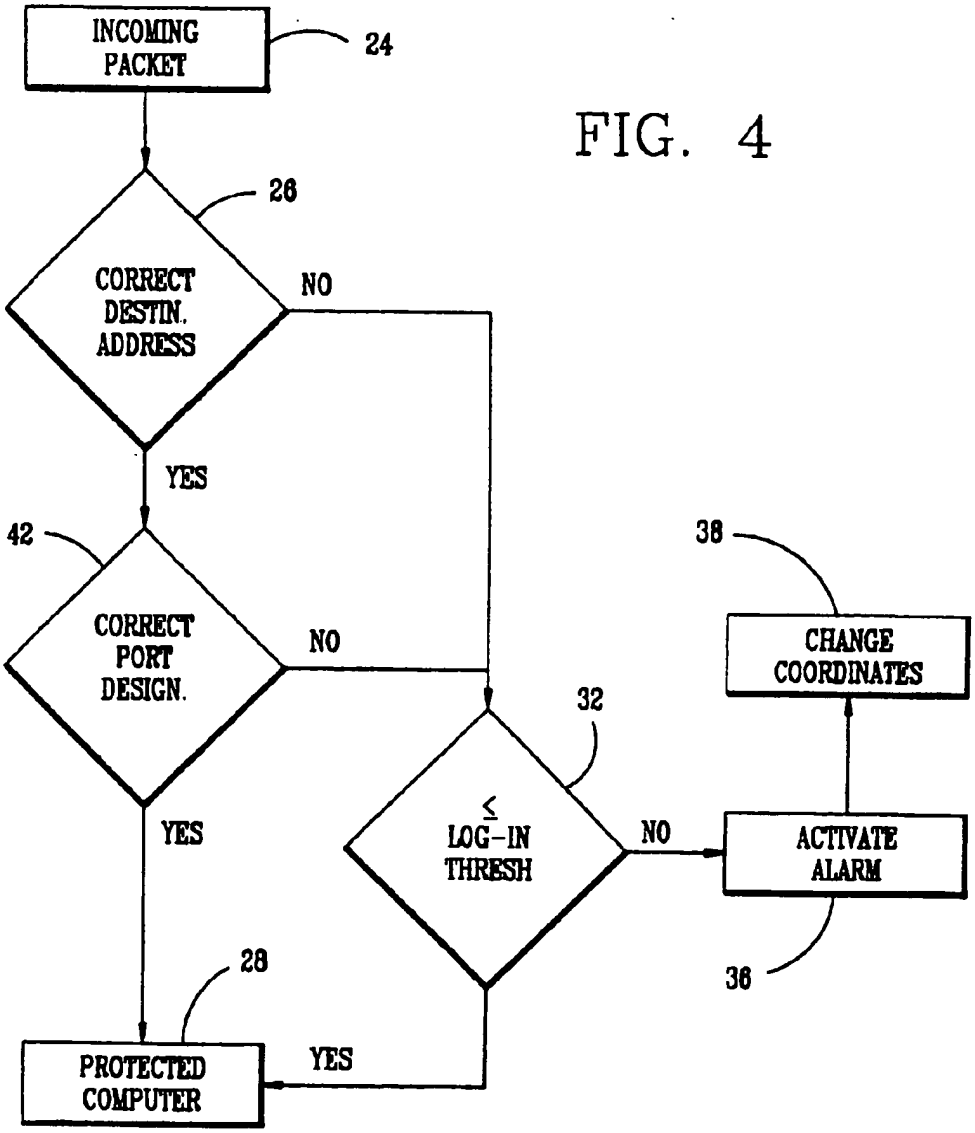


FIG. 4

Petitioner Apple Inc. - Exhibit 1002, p. 293

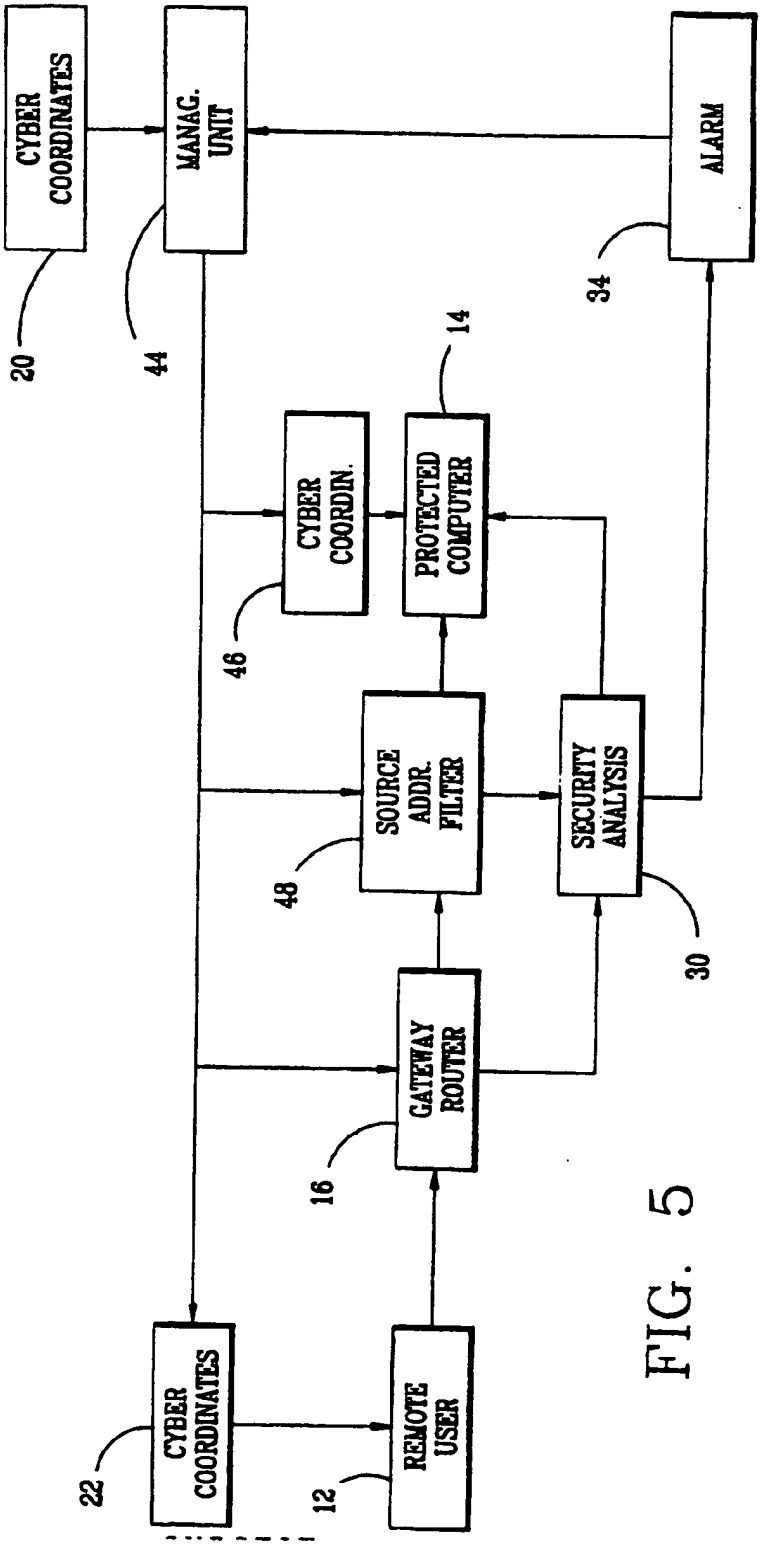

CYBER COORDINATES
MANAG. UNIT
ALARM
20
44
34
14
CYBER COORDIN.
PROTECTED COMPUTER
46
SOURCE ADDR. FILTER
SECURITY ANALYSIS
48
30
GATEWAY ROUTER
16
CYBER COORDINATES
REMOTE USER
22
12

FIG. 5

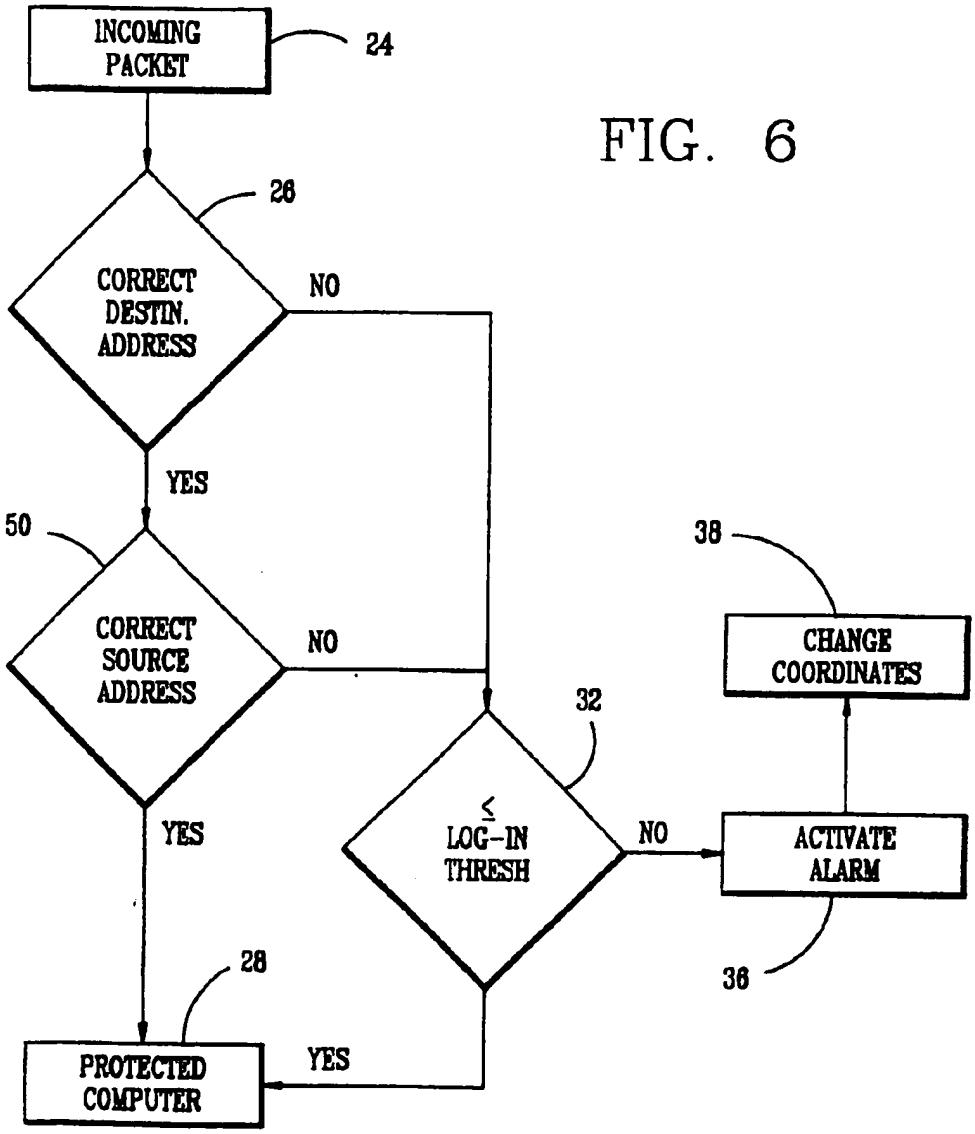
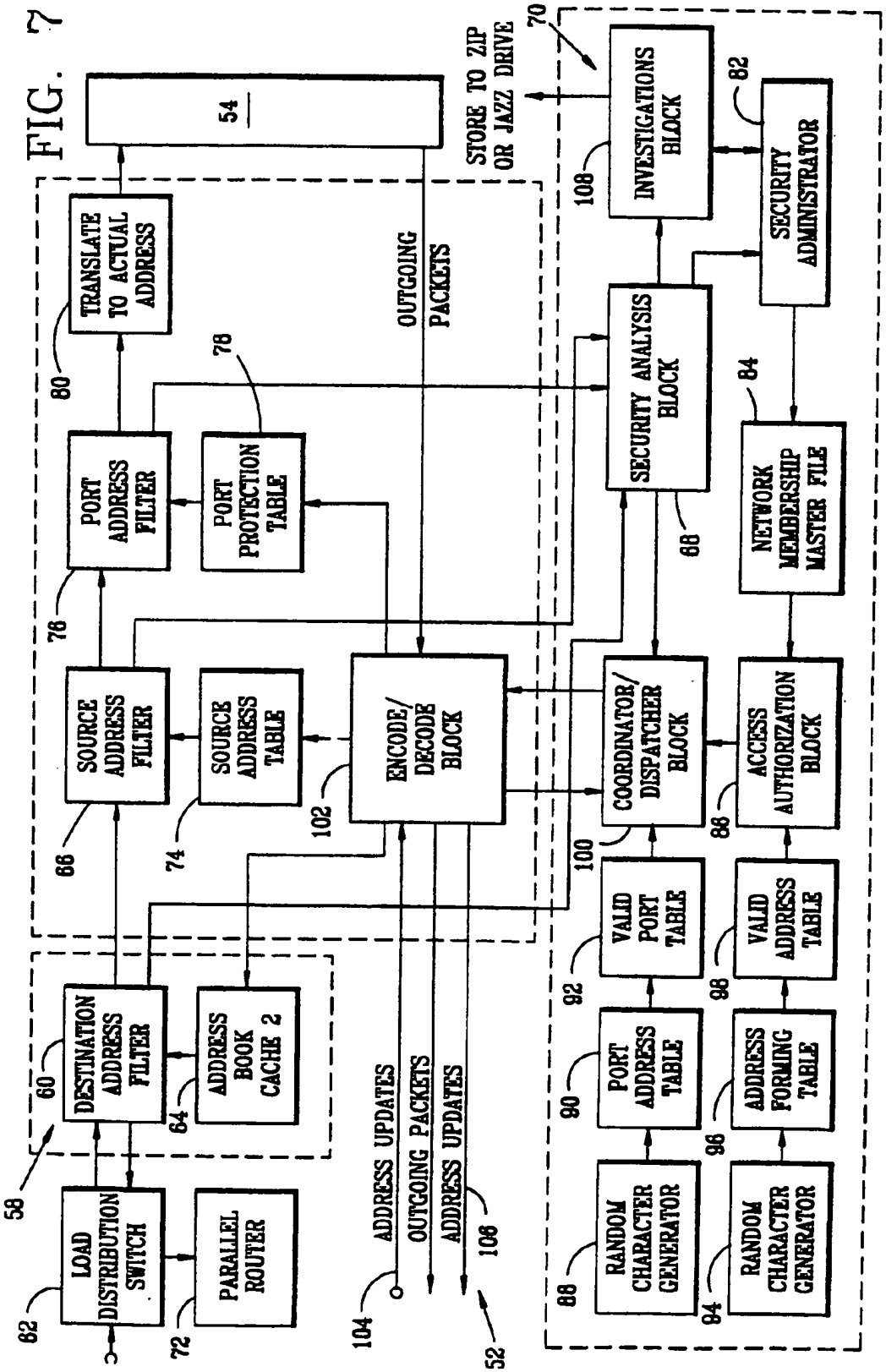


FIG. 6

Petitioner Apple Inc. - Exhibit 1002, p. 295

FIG. 7


54
STORE TO ZIP OR JAZZ DRIVE
70
INVESTIGATIONS BLOCK
108
82
SECURITY ADMINISTRATOR
TRANSLATE TO ACTUAL ADDRESS
80
OUTGOING PACKETS
78
SECURITY ANALYSIS BLOCK
84
NETWORK MEMBERSHIP MASTER FILE
PORT ADDRESS FILTER
PORT PROTECTION TABLE
76
68
SOURCE ADDRESS FILTER
SOURCE ADDRESS TABLE
ENCODE/ DECODE BLOCK
COORDINATOR/ DISPATCHER BLOCK
ACCESS AUTHORIZATION BLOCK
66
74
102
100
86
VALID PORT TABLE
VALID ADDRESS TABLE
92
98
DESTINATION ADDRESS FILTER
ADDRESS BOOK CACHE 2
60
64
PORT ADDRESS TABLE
ADDRESS FORMING TABLE
90
96
58
LOAD DISTRIBUTION SWITCH
PARALLEL ROUTER
ADDRESS UPDATES
OUTGOING PACKETS
ADDRESS UPDATES
RANDOM CHARACTER GENERATOR
RANDOM CHARACTER GENERATOR
62
72
104
106
52
88
94

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/08219

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) :G06F 11/00
US CL : 713/201
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/201,200,202; 340/825.31,825.34; 380/255;

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
APS US PATENT FILE; WEST; JPAB; EPAB; DWPI; TDBD;

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,805,801 A (HOLLOWAY ET AL) 08 SEPTEMBER 1998, Entire document.	1-25
Y	US 5,796,942 A (ESBENSEN) 18 AUGUST 1998, Entire document.	1-25
Y,P	US 5,905,859 A (HOLLOWAY ET AL) 18 MAY 1999, Entire document.	1-25
Y	US 5,892,903 A (KLAUS) 06 APRIL 1999, Entire document.	1-25
A	US 5,537,099 A (LIANG) 16 JULY 1996, Entire document.	1-25
A	US 5,278,901 A (SHIEH ET AL) 11 JANUARY 1994, Entire document.	1-25

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 20 JULY 2000	Date of mailing of the international search report 22 AUG 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer NADEEM IQBAL Telephone No. (703) 308-5228

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/08219

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,P	US 5,991,881 A (CONKLIN ET AL) 23 NOVEMBER 1999, Entire document.	1-25

Form PCT/ISA/210 (continuation of second sheet) (July 1998)*

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

CORRECTED VERSION

B1002

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 March 2001 (08.03.2001)

PCT

(10) International Publication Number
WO 01/016766 A1

(51) International Patent Classification[7]: G06F 13/00

(21) International Application Number: PCT/US00/23774

(22) International Filing Date: 31 August 2000 (31.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/151,563 31 August 1999 (31.08.1999) US

(71) Applicant: SCIENCE APPLICATIONS INTERNATIONAL CORPORATION [US/US]; 10260 Campus Point Drive, San Diego, CA 92121 (US).

(72) Inventors: WHITTLE, Bryan; 73 Zion-Wortsville Road, Skillman, NJ 08558 (US). TESINK, Kaj; 140 Park Road, Fair Haven, NJ 07704 (US).

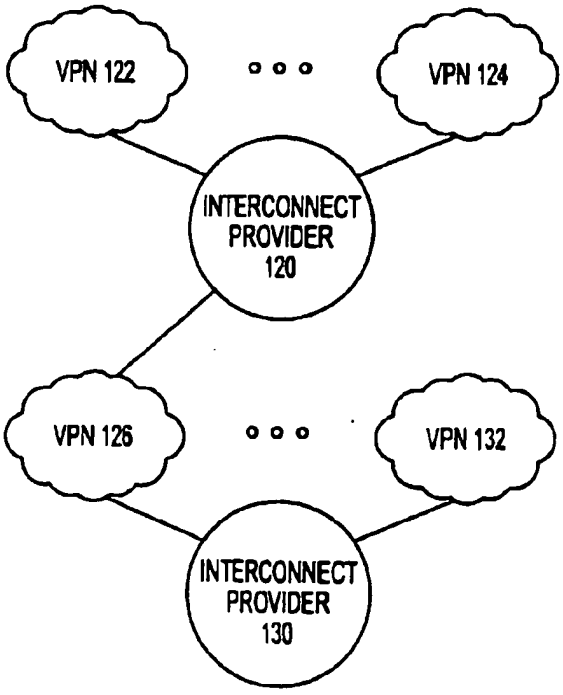
(74) Agents: ROBINSON, Douglas, W. et al.; Banner & Witcoff, Ltd., Eleventh Floor, 1001 G Street, N.W., Washington, D.C 20001-4597 (US).

(81) Designated States *(national)*: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR INTERCONNECTING MULTIPLE VIRTUAL PRIVATE NETWORKS



(57) Abstract: A system and method for interconnecting multiple VPNs (122, 124, 126, 132), each using multiple service providers (120, 130), while offering a minimum standard of end-to-end connection quality and reliability. The system and method utilizes an overseer that resolves end-to-end issues across multiple interconnected virtual private networks (122, 124, 126, 132). When connecting multiple virtual private networks (122, 124, 126, 132) multiple interconnect providers (120, 130) are interconnected so that the end-to-end service quality standard. The certification of service providers, exchange points, transit service providers and IPSec devices permits interoperability for encryption, integrity and authentication across the product of all IPSec vendors. When two subscribers both use certified IPSec equipment then they can provide each other with controlled access to each other's networks.

WO 01/016766 A1

Published:
— *with international search report*

(48) Date of publication of this corrected version:
12 September 2002

(15) Information about Correction:
see PCT Gazette No. 37/2002 of 12 September 2002, Section II

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR INTERCONNECTING MULTIPLE VIRTUAL PRIVATE NETWORKS

This application claims priority to the following provisional patent applications, which are incorporated herein by reference in their entireties:

(1) Provisional Application Serial No. 60/151,563, titled "Method & Apparatus For a Globalized Automotive Network & Exchange," filed on August 31, 1999, and having reference no. 99,532 (479.83581).

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to virtual private networks. More particularly, the present invention relates to virtual private networks wherein in each virtual private network, multiple service providers can be utilized by the trading partners of the virtual private network. The end-to-end service quality of the connection within the virtual private network is guaranteed to meet minimum requirements. The end-to-end service quality encompasses numerous factors including: network services; interoperability; performance; reliability; disaster recovery and business continuity; security; customer care; and trouble handling. The system and method of the present invention is directed to the interconnection of multiple virtual private networks each having multiple service providers. Furthermore the present invention encompasses a system and method for interconnecting multiple interconnect providers, such as exchange points, exchange networks, direct connect or transit service providers, between the multiple virtual private networks. Finally, the present invention employs an end-to-end overseer across the multiple virtual private networks.

Description of the Related Art

Early in 1994, the automotive industry recognized the need for global network services that would support more new demanding automotive business applications. The purpose of this network service was to simplify complex, redundant, outdated connection methods while minimizing costs and ensuring the management, security, reliability, and performance essential to the automotive industry. Transport Control Protocol/Internet Protocol (TCP/IP) was endorsed as the standard suite for electronic data communications.

Petitioner Apple Inc. - Exhibit 1002, p. 301

Ultimately in 1995, the industry formed a Telecommunications Project Team to oversee the design and development of a common global communication infrastructure supporting automotive industry application initiatives (later called the Automotive Network eXchange (ANX) Implementation Task Force). The Task Force, in June 1997, published the initial results of the technical design process for this new network service, called the Automotive Network eXchange (ANX), in "ANX Release 1 Draft Document Publication" (TEL-2 01.00). This reference is incorporated herein by reference in its entirety. The TEL-2 specification undergoes constant updating and correction.

The ANX system is a business-to-business communications infrastructure that provides a uniform, secured link between trading partners, such as manufacturers and suppliers, in the automotive industry. The ANX is a subscription-based network composed of Certified Service Providers (CSP). CSPs are providers of IP network service that have satisfied certain service end-to-end quality. CASPs are certificate authority service providers. The Certified Exchange Point Operator (CEPO) provides services to interconnect CSPs. CEPOs also must satisfy certain end-to-end service quality requirements.

Trading Partners (TP) are registered end users, or subscribers, of the ANX system such as automotive parts manufacturers, suppliers, original equipment manufacturers, and car manufacturers. The ANX system allows TPs to communicate, exchange information, and transact business with other TPs over the ANX network. The TP may utilize any TCP/IP-compliant application program to exchange information with other TPs. The registered TP selects the TPs with which it wants to communicate and thereafter may gain access to and receive communications from those selected TPs. As a result, the ANX system allows each TP to develop its own virtual private network with its customers and vendors.

The ANX system significantly reduces the complexity of connecting to multiple trading partners. Since there are diverse communication protocols for the trading partners, separate links are required to access each trading partner.

By having a single private network operated under a uniform protocol, interconnectivity between various trading partners is substantially simplified. In addition, ANX offers improved end-to-end service quality. For example, if an auto manufacturer needs to place with its parts supplier an order for car seats, the

Petitioner Apple Inc. - Exhibit 1002, p. 302

manufacturer may submit over the ANX system its confidential CAD drawings directly to the supplier. The manufacturer may also fill out the order form that the supplier may have for filling orders and timely submit over the ANX system due to its high reliability and performance.

The CSP and the CEPO must satisfy certain performance and security requirements in order to be certified under the ANX. The certification process is disclosed in ANX Release 1 Document Publication (TEL-2 02.00), which is incorporated herein by reference in its entirety.

The ANX VPN permits the use of a plurality of different IPSec devices. By virtue of the TEL-2 specification and the certification process all of the designated IPSec device are guaranteed to communicate with one another across the ANX VPN.

While the ANX was originated out of the need to interconnect automotive related companies, it is not limited to that industry. Any company/industry may become a TP, e.g. an aerospace company, a healthcare company, etc. ANX has become known as the Advanced Network eXchange.

With the advent of the Internet, global communication has become a reality. While the Internet works well for non-mission critical applications, such as transmitting and receiving e-mail and hosting websites, it has some drawbacks for business-to-business commerce and communication that require stringent end-to-end service quality. Quality concerns are in the area of end-to-end service quality as explained previously.

For example, when two companies want to communicate over the Internet, the lag between the systems at each company will be different virtually every time. The connection each has through their service provider, i.e. 14.4K, 28.8K, 56K, ISDN, DSL, T1, etc., plus the number of servers through which the connection is directed contribute to the resulting time lag between the two companies. Depending upon the type of information transmitted, the two parties may require a maximum acceptable time lag. Due to the nature of the Internet, it cannot guarantee such a maximum time lag. Furthermore, the two companies may desire that service assistance be available at certain times or 24 hours a day. The Internet has no such guarantees for help availability in a multi-provider environment. Such a lack of guaranteed bandwidth, latency and reliability are major impediments to business-to-business commerce and communication over the Internet.

Petitioner Apple Inc. - Exhibit 1002, p. 303

In recent years the number of electronic viruses and hacker attacks has increased dramatically. A company considering conducting business-to-business commerce over the Internet runs the risk of making their intranet vulnerable to such viruses and attacks with the potential related loss of data.

In order to address the security issue, some companies have developed virtual private networks (VPNs). Secure VPNs permit a company to communicate with any other entity on the network without the risk of increased vulnerability to viruses and hackers. However, while VPNs can connect to other VPNs over the Internet by providing authentication, access control, confidentiality and data integrity, there is still no way the end-to-end quality of the connection can be guaranteed to meet a required set of minimum standards in a multi-provider setting.

A secure VPN is a communication network that is secured with encryption and authentication. Secure VPNs are based on multiple technologies, for example IPSec, tunneling, certification and shared secret authentication. IPSec is the security standard established by the Internet Engineering task Force (IETF). Tunneling permits private networks to cross the Internet using unregistered IP addresses.

SUMMARY OF THE INVENTION

From the foregoing, it is desirable to provide a system and method for interconnecting multiple VPNs each using multiple service providers while offering a minimum standard of end-to-end service quality.

The system and method of the present invention utilizes an overseer that defines the service quality, continually qualifies service providers as meeting that service quality, and resolves end-to-end issues across multiple interconnected virtual private networks, such as the ANX. When connecting multiple virtual private networks according to the system and method of the present invention multiple interconnect providers are interconnected, and the manner in which these interconnect providers are interconnected so that the quality and reliability standards is met are another aspect of the present invention.

Certification of IPSec devices permits interoperability for encryption, integrity and authentication across the product of all IPSec vendors. When two subscriber companies both use certified IPSec equipment then they can provide each other with controlled access to each other's networks.

Petitioner Apple Inc. - Exhibit 1002, p. 304

Based on the foregoing, an object of the present invention is to provide a system and method of interconnecting multiple VPNs each using multiple service providers while offering a minimum standard of end-to-end connection quality and reliability.

Another object of the present invention is to provide a system and method of interconnecting multiple VPNs having an overseer that resolves end-to-end issues across multiple virtual private networks.

Still another object of the present invention is to provide a system and method of connecting multiple virtual private networks in which multiple interconnect providers are interconnected so that the end-to-end service quality is met.

DETAILED DESCRIPTION OF THE DRAWINGS

The foregoing and other attributes of the present invention will be described with respect to the following drawings in which:

Fig. 1 is a block diagram of two interconnected virtual private networks according to the present invention;

Fig. 2 is a configuration of governance and management of separate virtual private networks;

Fig. 3 is a configuration of governance and management of interconnected virtual private networks according to the present invention;

Fig. 4 is an interconnection configuration for governance of multiple interconnected virtual private networks according to the present invention;

Fig. 5 is a flow chart showing contractual obligations according to the present invention;

Fig. 6 is a diagram illustrating end-to-end latency in a virtual private network having multiple service providers;

Petitioner Apple Inc. - Exhibit 1002, p. 305

Fig. 7 is a diagram illustrating end-to-end availability in a virtual private network having multiple service providers;

Fig. 8 is a diagram illustrating trouble handling in a virtual private network having multiple service providers;

Fig. 9 is a diagram illustrating an accountability model for a single virtual private network having multiple service providers;

Fig. 10 is a diagram illustrating an accountability model for multiple virtual private networks having multiple service providers according to the present invention;

Fig. 11 is a diagram illustrating end-to-end interconnection of two virtual private networks according to the present invention;

Fig. 12 is a diagram illustrating a trouble escalation model for interconnection of two virtual private networks according to the present invention;

Fig. 13 is a diagram illustrating a multiple virtual private network fee model for interconnection of two virtual private networks according to the present invention; is a diagram illustrating interconnection of two virtual private networks using a multiple transit certified service providers according to the present invention;

Fig. 14 is a diagram illustrating interconnection of two virtual private networks using a single transit certified service provider according to the present invention;

Fig. 15 is a diagram illustrating interconnection of two virtual private networks using a multiple transit certified service providers according to the present invention;

Figs. 16 is a diagram illustrating interconnection of multiple virtual private networks using a multiple transit certified service providers, where no single transit

Petitioner Apple Inc. - Exhibit 1002, p. 306

certified service provider connects all of the virtual private networks according to the present invention; and

Figs. 17a - c are alternative configurations for interconnecting multiple virtual private networks according to the present invention.

Petitioner Apple Inc. - Exhibit 1002, p. 307

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Fig. 1 shows a block diagram of two interconnected virtual private networks 20 and 22. The present system and method of the interconnecting multiple virtual private networks is not intended to be limited to only these types of networks and has applicability to a wide variety of virtual private networks.

Each virtual private network 20 and 22 is shown having a trading partner (TP) 24 and 26, respectively. While Fig. 1 shows only one TP 24 and 26 for each virtual private network, there can in fact be hundred or thousands of such TPs for each virtual private network. Fig. 1 is intended to define the end-to-end service quality concept, and for such a purpose, only one TP 24 and 26 is need for each virtual private network 20 and 22.

The end-to-end service quality, provided by the present system and method of interconnecting multiple virtual private networks, cannot be achieved by simply interconnecting two virtual private networks, such as 20 and 22, with a wire. The end-to-end service quality incorporates a user-centric philosophy, where the user is the TP or subscriber. The user is guaranteed a minimum level of service encompassing factors that include: network services; interoperability; performance; reliability; disaster recovery and business continuity; security; customer care; and trouble handling. Simply connecting the two virtual private networks 20 and 22 with a wire will not achieve the minimum satisfactory levels for these factors.

To achieve such minimum levels of satisfactory performance for these factors the system and method must include a way to resolve disputes between the two virtual private networks. Referring to Fig. 2, each VPN 20 and 22 is shown as having its own governance, program management, coopetition policy, contracts, service assurance, and service description. While each virtual private network can operate with a successful level of end-to-end service quality when each VPN is not interconnected to another VPN, the governance, program management, coopetition policy, contracts, service assurance, and service description may need to be revised when interconnecting two or more VPNs in order to maintain the end-to-end service quality. It will be appreciated that at the very least the interconnection of at least two VPNs adds at least one additional level of complexity with regard to service between the VPNs.

Petitioner Apple Inc. - Exhibit 1002, p. 308

One resolution is shown in Fig. 3, in which each VPN 20 and 22 maintain their own governance, but the program management, coopetition policy, contracts, service assurance, and service description for the two VPNs 20 and 22 are unified. Such unification means that where the parameters for the program management, coopetition policy, contracts, service assurance, and service description of the two VPNs 20 and 22 are different, the parameter used in one of the networks is chosen as the acceptable minimum standard or a compromise parameter different from the parameter used in each or the VPNs is agreed upon. It is possible that the parameters for communication within each VPN need not change, while the new parameters are used only when communicating between VPNs. Fig. 3 further shows that the system and method contemplate connecting more than two VPNs.

One configuration for governance of multiple interconnected VPNs is shown in Fig. 4. In this scenario each VPN has its own program overseer (POVER) 30, and a global, or multiple virtual private network, overseer 32 is provided to resolve issues between the POVERs 30. Arrows are shown between the POVERs 30 indicating that the POVERs 30 are free to resolve their issues without requiring the GOVER 32. The GOVER is called on when direct POVER-to-POVER resolution fails. Each of the POVERs 30 governs one of the regional VPNs, while the GOVER 32 oversees the interconnection of the VPNs.

The GOVER is responsible for end-to-end quality assurance, and in particular acts as an inter-VPN interconnection certifier. The GOVER certifies interconnection facilities, and certifies a global CASP-CASP trust model. The GOVER also is an inter-VPN arbitrator that steps in when POVERs cannot resolve trouble between them.

Since the VPNs are used to running their networks in isolation, the interconnection of multiple VPNs has unique issues such as resolving trouble and conflicts between the VPNs and maintenance of minimum end-to-end service quality across the multiple programs. Since the system and method of the present invention are directed to providing specific end-to-end service quality, it must be possible for TPs to quantify the end-to-end service quality levels, and these service quality levels must be sufficient to allow applications to work across the multiple VPNs. Therefore, a high level of metric compatibility and measurement techniques are required.

Petitioner Apple Inc. - Exhibit 1002, p. 309

In the ANX type VPN each TP, CSP and CEP must meet specified criteria to become certified and to maintain that certification. The certification provides the TPs or subscribers with confidence that the level or transport and security will meet their business needs. The ANX type VPN utilizes multiple CSPs. On one level it is easier to run a VPN where all TPs are required to use a single CSP. The use of multiple CSPs in the ANX type VPN fosters competition between the CSPs and allows the VPN to reach TPs that may not be serviced by a single CSP. The implementation of multiple CSPs, however, brings with it the drawback of insuring that the CSPs can talk to one another. Whether the connection from one TP to another TP within the same VPN is through a single CSP of two CSPs should be invisible to the TPs. The TPs need never know when one or more CSPs are used for any particular connection. The certification process ensures that the TPs use one of the certified IPSec devices at their premises, and that the CSPs will utilize certified equipment and meet certain metrics so as to achieve the end-to-end service quality guaranteed to the TPs. In this manner, the multiple CSPs will be able to communicate with one another. The CSPs must meet business criteria, technical metrics, ongoing monitoring, trouble-handling criteria, routing registry criteria, and domain name registry criteria to achieve and maintain certification.

Fig. 5 shows the contractual obligations of the members of an ANX-type VPN. The TPs 40 contract with the VPN, as denoted in Fig. 5 by the arrows to the overseer 50, and contract with one of the multiple CSPs 42. The CSPs contract with the VPN and with the CEPO 44. The CEPO 44 contracts with the VPN. Each entity is responsible for the services that that entity provides.

The technical metrics for achieving end-to-end service quality in the ANX-type network include among other metrics, latency and availability. Fig. 6 illustrates the end-to-end latency within the ANX network. The TP1 router 60 is connected to ANX CSP_1 62, which in turn is connected to ANX CEPO 64. TP2 router 66 is connected to ANX CSP_2 68, which is connected to ANX CEPO 64. The packet latency from each router 60 and 66 through the corresponding CSP is 125 msec. The latency through the ANX CEPO is on the order of microseconds. The total packet latency through the network is therefore only slightly more than 250 msec.

Fig. 7 illustrates the end-to-end availability metric. The Access network between the TP1 router 60 and the ANX CSP_1 62 is permitted to be unavailable 43.80

Petitioner Apple Inc. - Exhibit 1002, p. 310

hours/year. The ANX CSP_1 62 may only be unavailable 2.63 hrs./year. The trunk 65 between the ANX CSP_1 62 and the ANX CEPO may only be unavailable 1.76 hrs./year. The ANX CEPO may only be unavailable 0.44 hours/year. The foregoing availabilities yield a total of 99.895% availability or 9.22 hours per year downtime.

The outline for how trouble is handled within the ANX-type VPN is shown in Fig. 8. There are effectively five layers of trouble handling. At the first level trouble between TPs is handled directly between the two TPs. Similarly, issues between the TPs and the CSPs are handled between the two parties. CSPs and the CEPOs also resolve their troubles between the troubled parties. A network overseer is provided to handle troubles that cannot be handled in the foregoing scenarios. The overseer can take complaints from the TPS, the CSPs, and the CEPOs.

A key to providing predictable end-to-end service quality is that the TPs must know the level of service they receive. To this end four service provider accountability levels exist. First, service providers, both interconnect providers and CSPs, must timely fix infrequent service provider troubles. Second, there must be end-to-end service provider cooperation to handle any troubles. Third, recourse must be provided to resolve disputes in the event of disagreement between CSPs and/or interconnect providers. Fourth, recourse must be provided to resolve continued non-compliance with the end-to-end service quality.

Referring to Figs. 9 and 10, charts for single VPN and interconnected VPNs are shown, respectively. In Fig. 9, the CSPs 70, CEPOs 72 and CASPs 74 are accountable to the POVER 76. The POVER 76 is accountable to the body 78 representing the TPs. The body 78 is accountable a regional/national arbitration body 80. Where multiple VPNs are interconnected in Fig. 10, the CSPs 70, the CEPOs 72, and CASPs 74 are accountable to the POVERs 76. The POVERs 76 are accountable to a GOVER 77, which in turn is accountable to the body 78. The body 78, instead of being accountable to the regional/national arbitration body 80, is accountable to an international arbitration body 82.

The GOVER/POVER model is but one way to oversee ensuring of the end-to-end service quality and metric compatibility. How the ANX-type networks are connected will be discussed below. In this context there must be five key types of end-to-end technology compatibility: 1 network interconnection that ensures a trading partner on one VPN can reach any trading partner on the other VPN; 2 routing

Petitioner Apple Inc. - Exhibit 1002, p. 311

compatibility that ensures any trading partner on one VPN can logically reach nay TP on the other VPN; 3 naming compatibility, e.g. so the web names or e-mail names of any trading partner on one VPN can be resolved to an address that is routable over the two VPNs; 4 IPSec compatibility; and 5 digital security certificate compatibility across multiple VPNs. While Figs. 9 and 10 refer to regional/national VPNs and international arbitration, the VPNs need not be limited to a specific country or geographical area. Any ANX-type VPN, regardless of the location of its subscribers could be interconnected.

While Fig. 1 illustrated the interconnection of two VPNs 20 and 22, a significant element is missing. Fig. 11 shows two VPNs, that have multiple service providers, which are connected through an inter-program service provider, also called an interconnect provider. The Tel-2 specification is still used as the basic guide in determining the end-to-end service quality, however regional or particular VPN peculiarities, referred to as deltas, must be considered when establishing the interconnected end-to-end service quality standards.

Returning to the GOVER/POVER model for overseeing interconnected VPNs; Fig. 12 illustrates an end-to-end trouble escalation model. It is expected that CSPs will work together to resolve trouble before contacting a POVER. Similarly, the POVERs and/or the POVERS and the interconnect provider are expected to work together to resolve trouble before contacting the GOVER.

When expanding from a single VPN to interconnected VPNs the inherent costs of running the system naturally increase. How such costs are distributed is an important part of the system. As shown in Fig. 13, the POVERs 100 pay fees to the GOVER to offset the costs of maintaining the GOVER. The VPNs having multiple service providers in turn pay fees to support the POVER. Furthermore the interconnect providers pay a certification fee to the GOVER for certification as a interconnect provider between VPNs.

There are multiple methods of interconnecting multiple VPNs with interconnect providers. As shown in Fig. 14, all the VPNs, having multiple service providers, can be interconnected using a single interconnect provider. Alternatively, all the VPNs can be interconnected by multiple interconnect providers, as shown in Fig. 15, thereby creating competition between the interconnect providers, just as there is competition between the CSPs in a single xNX-type VPN. Finally, as shown in

Petitioner Apple Inc. - Exhibit 1002, p. 312

Fig. 16, where no suitable interconnect provider is available to connect all he VPNs having multiple service providers, multiple interconnect providers are used. These interconnect providers service different combinations of VPNs. In Fig. 16, interconnect provider 120 interconnects VPNs having multiple service providers 122, 124, and 126. Interconnect provider 130 interconnects VPNs having multiple service providers 132 and 126. As a result, a TP of VPN 132 must connect through both Interconnect provider 130 and Interconnect provider 120 to reach TPs of either VPN 122 or 124.

How the multiple VPNs interconnect will directly affect the resulting end-to-end service quality. Figs. 17a-c illustrate potential configurations of multiple VPNs. In Fig. 17a a first TP 200 connects to a first CSP 210. The CSP210 connects to a first exchange point 220. The TP 200, CSP 210, and the exchange point 220 are within a first VPN 240. A second TP 250 connects to a second CSP 260, which connects to a second exchange point 270. The TP 250, CSP 260 and exchange point 270 are within a second VPN 280. The two VPNs 240 and 280 are interconnected by an Interconnect provider 300, which is connected to the exchange points 220 and 270.

In Fig. 17b TP 200, CSP 210, exchange point 220 and Interconnect provider 300 are connected in the same manner shown in Fig. 17a. While the second TP 250 is connected to the CSP 260, the exchange point 270 is not provided. Instead CSP 260 is shown as connecting directly to the Interconnect provider 300. This embodiment encompasses the situation where the Interconnect provider 300 and CSP 260 are the same entity or are directly wired. Fig. 17c is similar to Fig. 16b,
Except that the interconnect provider also acts as a CSP 320, and a third TP 310 is connected directly to the Interconnect provider 300/CSP 320.

As stated previously, while the end-to-end service quality is based upon the TEL-2 specification, the degree to which the TEL-2 specification needs to be modified to interconnect multiple VPNs depends upon the chosen complexity of the interconnection. An xNX-type VPN uses a maximum of two CSPs between any two TPS. A larger value, either three or four, is needed for multiple VPNs. The Interconnect provider will account for one additional CSP, and for configuration set forth in Fig. 16, two Interconnect providers are employed in addition to the two CSPs yielding four CSPs.

Petitioner Apple Inc. - Exhibit 1002, p. 313

Having described several embodiments of the system and method for interconnecting multiple virtual private networks in accordance with the present invention, it is believed that other modifications, variations and changes will be suggested to those skilled in the art in view of the description set forth above. It is therefore to be understood that all such variations, modifications and changes are believed to fall within the scope of the present invention as defined in the appended claims.

Petitioner Apple Inc. - Exhibit 1002, p. 314

What is claimed is:

1. A system of interconnecting multiple virtual private networks, each of said multiple private networks having multiple service providers, comprising:

at least one interconnect provider for connecting said multiple virtual private networks,

said multiple virtual private networks connected through said at least one interconnect provider having minimum standards for cross network services, virtual private network interoperability, inter–network performance, inter-network reliability, disaster recovery and business continuity, inter-network security, inter-network customer care, and inter-network trouble handling.

2. A system as recited in claim 1, further comprising a maximum acceptable latency between subscribers to different ones of said multiple virtual private networks.

3. A system as recited in claim 1, further comprising a maximum acceptable number of service providers between subscribers to different ones of said multiple virtual private networks.

4. A system as recited in claim 1, further comprising a minimum acceptable period of unavailability of interconnected multiple virtual private networks.

5. A system as recited in claim 1, wherein each of said multiple virtual private networks comprises a program overseer to ensure end-to-end service quality across each of said multiple virtual private networks.

6. A system as recited in claim 5, further comprising a global overseer to ensure end-to-end service quality across multiple ones of said multiple virtual private networks.

7. A system as recited in claim 6, wherein said global overseer resolves disputes between ones of said program overseers for said multiple virtual private networks or said program overseers and said at least one interconnect provider.

Petitioner Apple Inc. - Exhibit 1002, p. 315

8. A system as recited in claim 5, wherein said program overseer for each one of said multiple virtual private networks resolves disputes between service providers within said one of said multiple virtual private networks.

9. A system as recited in claim 6, wherein each of said program overseers and said multiple interconnect providers provides financial support to run said global overseer.

10. A system as recited in claim 1, wherein management of said multiple virtual private networks, contracts by between service providers and interconnect providers, service assurance, service description and how service providers and interconnect providers collaborate and compete are unified across said multiple virtual private networks to ensure end-to-end service quality.

11. A system as recited in claim 1, comprising multiple interconnect providers, wherein no one interconnect provider services all of said multiple virtual private networks.

12. A method of interconnecting multiple interconnection providers between multiple virtual private networks, each of said virtual private networks having multiple subscribers, multiple service providers and at least one exchange point interconnecting said multiple service providers, with guaranteed end-to-end service quality, comprising the steps of:

providing at least one interconnect provider disposed between a first set of said multiple service providers in one of said multiple virtual private networks and a second set of multiple service providers in a second one of said multiple virtual private networks.

13. A method of interconnecting multiple interconnection providers between multiple virtual private networks as recited in claim 12, wherein one of said at least one transit service providers is also one of said multiple service providers within at least one of said multiple virtual private networks.

Petitioner Apple Inc. - Exhibit 1002, p. 316

14. A method of interconnecting multiple interconnection providers between multiple virtual private networks as recited in claim 12, further comprising the step of certifying all of said multiple service providers in all of said multiple virtual private networks, said multiple transit service providers, and said exchange points to ensure minimum end-to-end quality and security levels are maintained.

15. A method of interconnecting multiple interconnection providers between multiple virtual private networks as recited in claim 12, comprising the further step of providing at least one exchange point between a first set of said multiple service providers in one of said multiple virtual private networks and said at least one interconnect service provider.

16. A method of interconnecting multiple interconnection providers between multiple virtual private networks as recited in claim 12, wherein a maximum number of service providers between two subscribers within one of said multiple virtual private networks is two, and the maximum number of said service providers and transit service providers between subscribers of different ones of said multiple virtual private networks is three.

17. A method of interconnecting multiple interconnection providers between multiple virtual private networks as recited in claim 15, further comprising the step of providing at least one second exchange point between a second set of said multiple service providers in another one of said multiple virtual private networks and said at least one transit service provider.

18. A system of interconnecting multiple virtual private networks, each of said multiple private networks having multiple service providers, comprising:

at least one interconnect provider for connecting said multiple virtual private networks,

each of said multiple virtual private networks comprising a program overseer to ensure end-to-end service quality across each of said multiple virtual private networks, and

Petitioner Apple Inc. - Exhibit 1002, p. 317

a global overseer to ensure end-to-end service quality across multiple ones of said multiple virtual private networks,

said multiple virtual private networks connected through said at least one interconnect provider have: minimum standards for cross network services; virtual private network interoperability; inter–network performance; inter-network reliability; disaster recovery and business continuity; inter-network security; inter-network customer care; and inter-network trouble handling.

19. A system as recited in claim 18, further comprising a maximum acceptable latency between subscribers to different ones of said multiple virtual private networks.

20. A system as recited in claim 18, further comprising a maximum acceptable number of service providers between subscribers to different ones of said multiple virtual private networks.

21. A system as recited in claim 18, further comprising a minimum acceptable period of unavailability of interconnected multiple virtual private networks.

22. A system as recited in claim 18, wherein said global overseer resolves disputes between ones of said program overseers for said multiple virtual private networks or said program overseers and said at least one interconnect provider.

23. A system as recited in claim 18, wherein said program overseer for each one of said multiple virtual private networks resolves disputes between service providers within said one of said multiple virtual private networks.

24. A system as recited in claim 18, wherein each of said program overseers and said multiple interconnect providers provides financial support to run said global overseer.

25. A system as recited in claim 18, wherein management of said multiple virtual private networks, contracts by between service providers and interconnect

Petitioner Apple Inc. - Exhibit 1002, p. 318

providers, service assurance, service description and how service providers and interconnect providers collaborate and compete are unified across said multiple virtual private networks to ensure end-to-end service quality.

26. A system as recited in claim 18, comprising multiple interconnect providers, wherein no one interconnect provider services all of said multiple virtual private networks.

Petitioner Apple Inc. - Exhibit 1002, p. 319

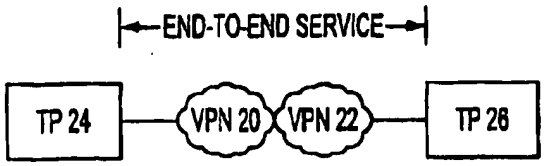


FIG. 1

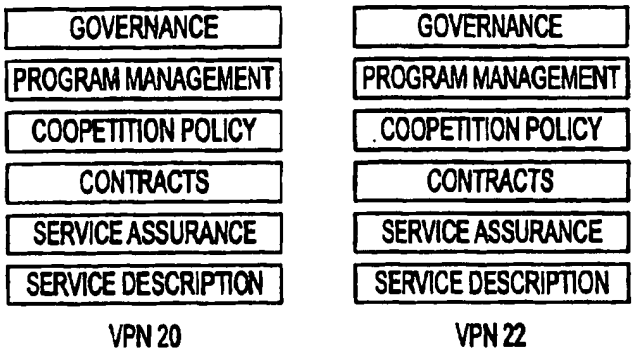


FIG. 2

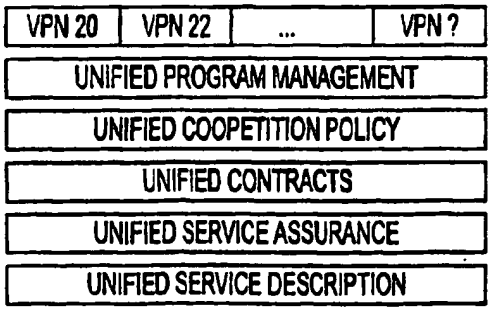


FIG. 3

Petitioner Apple Inc. - Exhibit 1002, p. 320

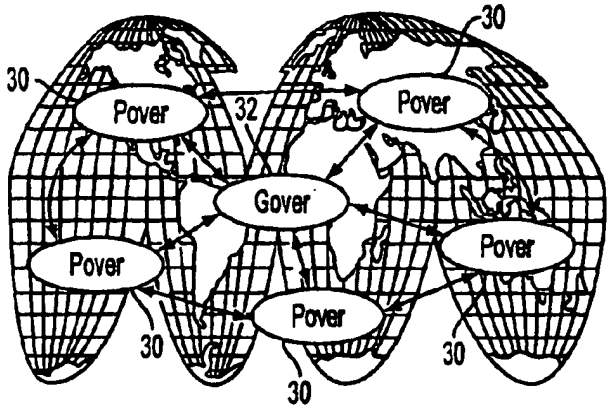


FIG. 4

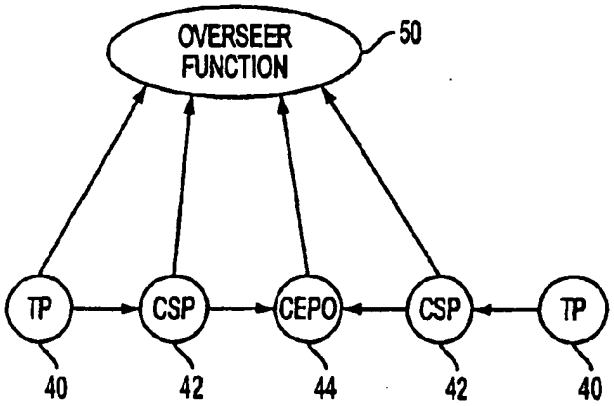


FIG. 5

Petitioner Apple Inc. - Exhibit 1002, p. 321

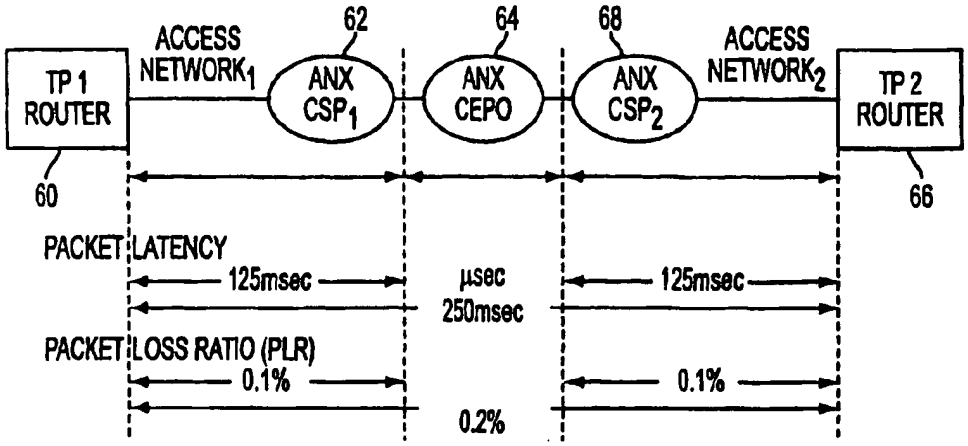


FIG. 6

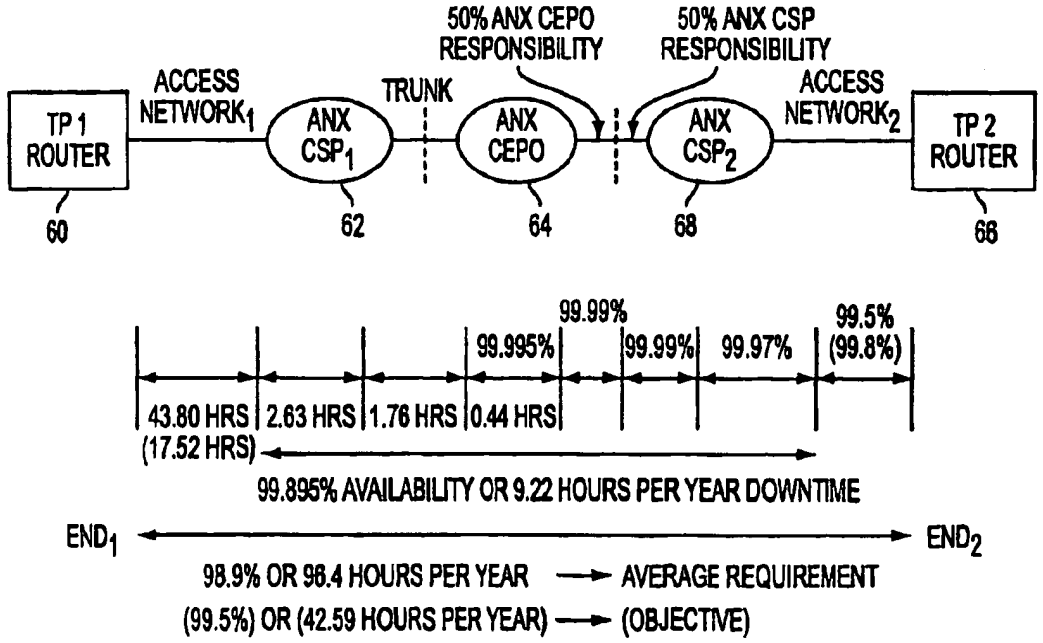


FIG. 7

Petitioner Apple Inc. - Exhibit 1002, p. 322

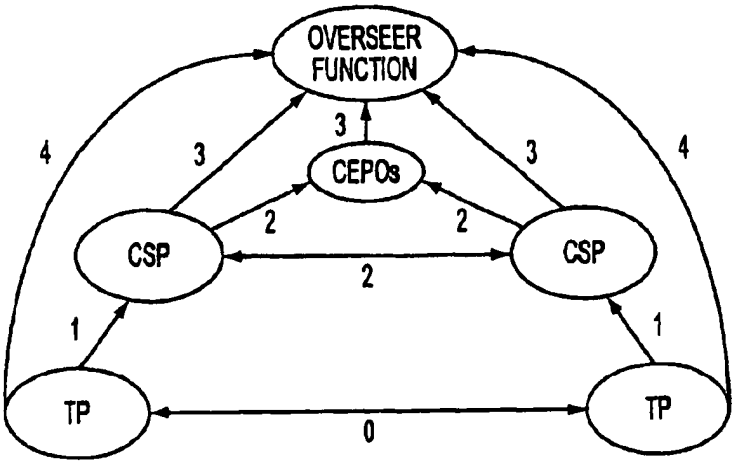


FIG. 8

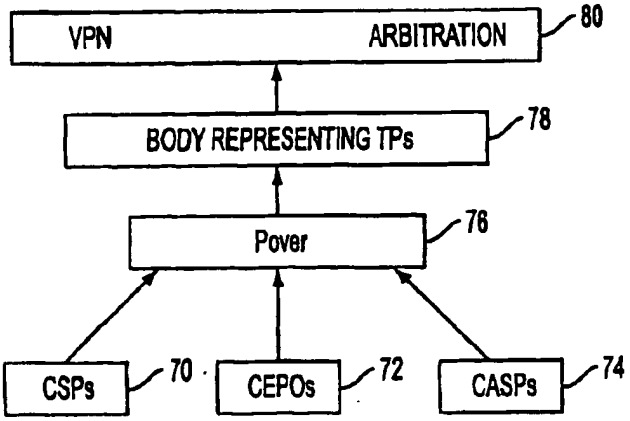


FIG. 9

Petitioner Apple Inc. - Exhibit 1002, p. 323

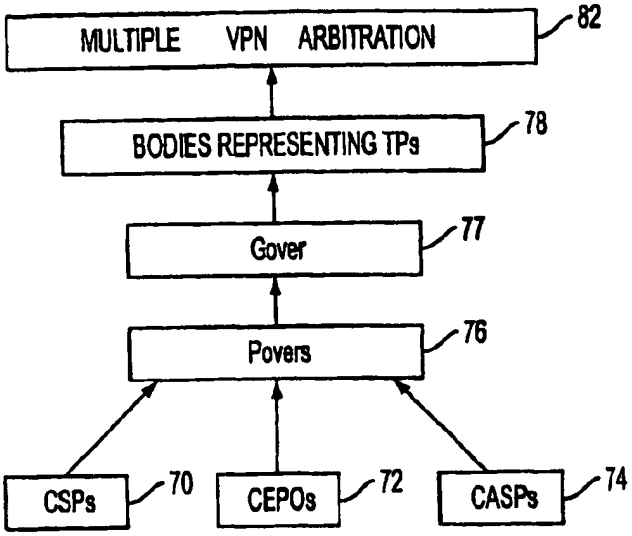


FIG. 10

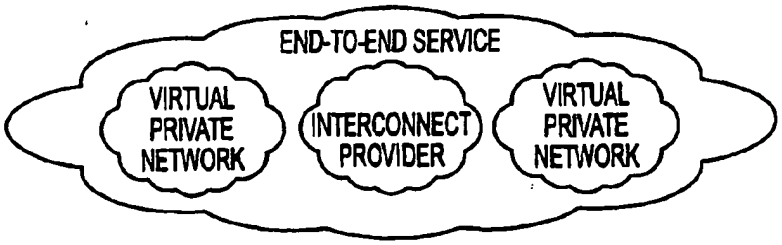


FIG. 11

Petitioner Apple Inc. - Exhibit 1002, p. 324

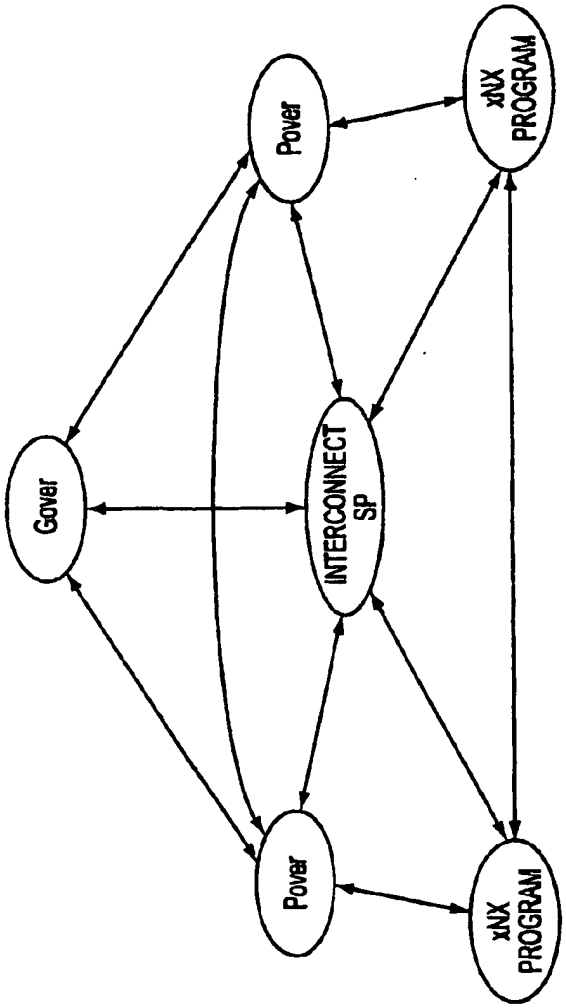


FIG. 12

Petitioner Apple Inc. - Exhibit 1002, p. 325

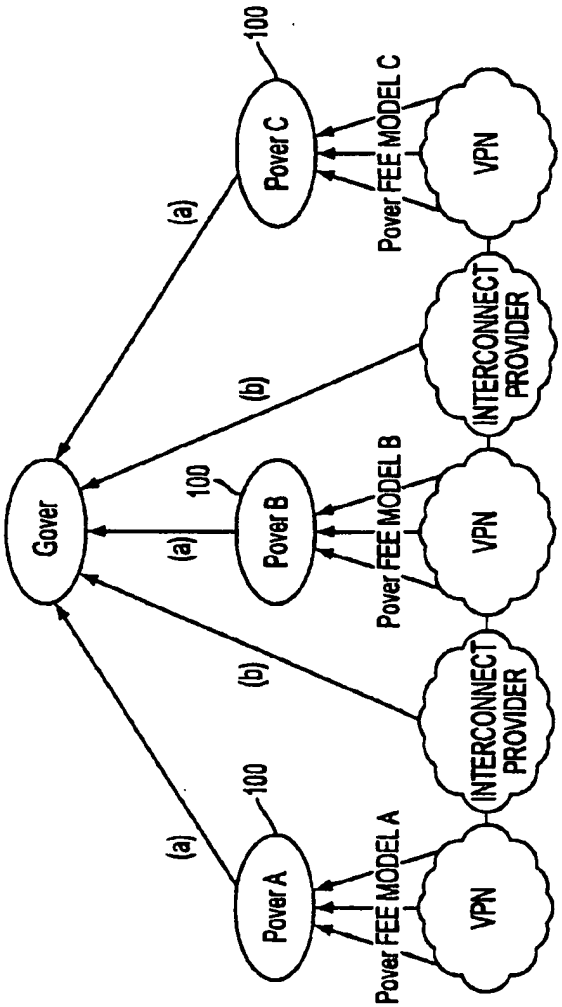


FIG. 13

Petitioner Apple Inc. - Exhibit 1002, p. 326

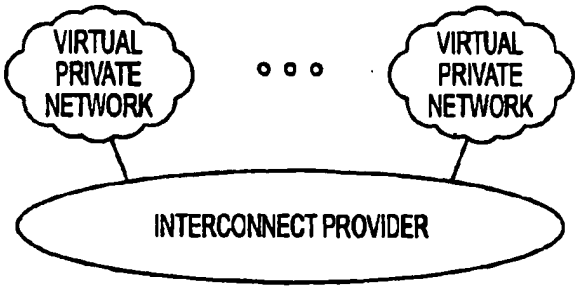


FIG. 14

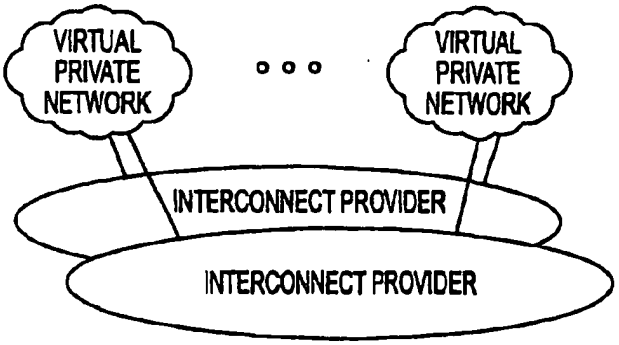


FIG. 15

Petitioner Apple Inc. - Exhibit 1002, p. 327

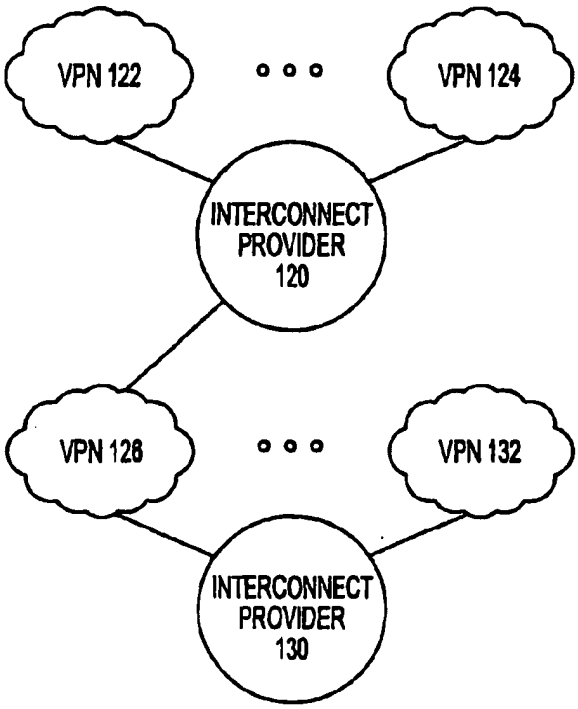


FIG. 16

Petitioner Apple Inc. - Exhibit 1002, p. 328

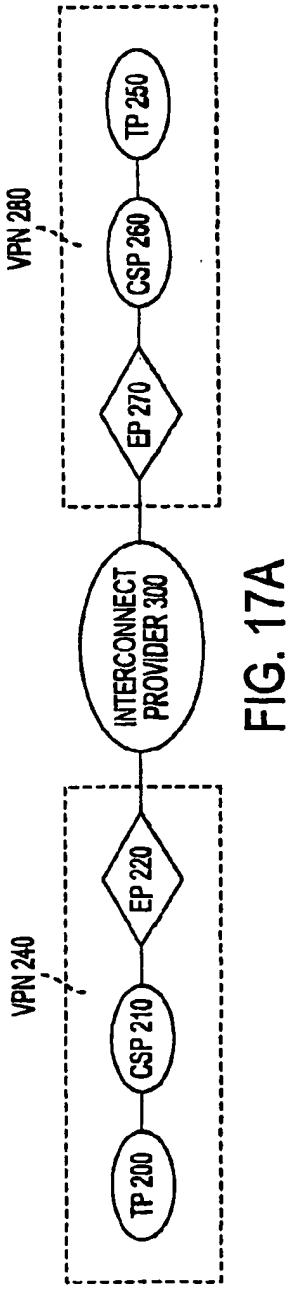


FIG. 17A

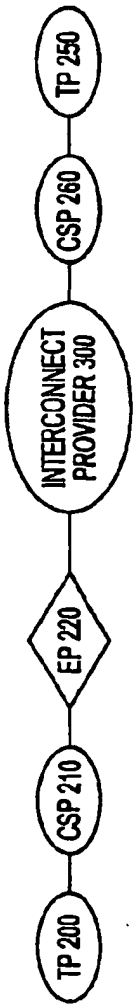


FIG. 17B

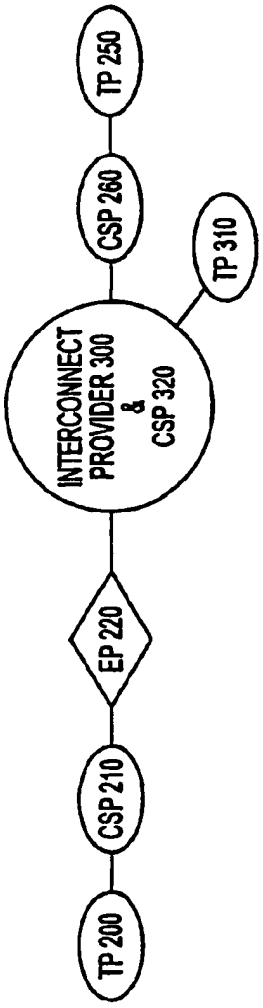


FIG. 17C

Petitioner Apple Inc. - Exhibit 1002, p. 329

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/23774

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) :G06F 13/00
US CL : 709/201, 220, 221, 223, 227, 228, 236, 238
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 709/201, 220, 221, 223, 227, 228, 236, 238

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CAS ONLINE
service(1w)providers, private(1w)(networks or lans), interconnection(1w)provider

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A, P	US 6,104,701 A (AVARGUES et al) 15 August 2000, Figs 1-3, col 1, lines 60-67, col 2, lines 1-6, lines 22-67, col 3, lines 1-6, col 6, lines 20-67, col 7, lines 1-26.	1-26

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
10 OCTOBER 2000	26 OCT 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer Peggy Harod MOUSTAFA M. MEKY Telephone No. (703) 305-9697

Form PCT/ISA/210 (second sheet) (July 1998)*

Attorney Docket No. 077580-0090

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Reexamination of:	)	
Edmund Munger, et al.	)	
	)	
U.S. Patent No.: 7,188,180	)	
Filed: November 7, 2003	)	**Examiner:**
Issued: March 6, 2007	)	**Andrew L. Nalven**
	)	
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK	)	**Group Art Unit: 3992**
	)	
Reexamination Proceeding	)	
Control No.: 95/001,270	)	
Filed: December 8, 2009	)	

PETITION FOR EXTENSION OF TIME UNDER 37 C.F.R. § 1.956 TO REPLY TO OFFICE ACTION IN REEXAMINATION

Mail Stop *INTER PARTES* REEXAM
Central Reexamination Unit
Office of Patent Legal Administration
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Pursuant to 37 C.F.R. § 1.956, the Patent Owner respectfully requests a two-month extension of time to respond to the Office Action mailed January 19, 2010 ("the Office Action"). The current deadline for response is March 19, 2010. A two-month extension would extend the deadline to May 19, 2010.

For reasons stated more fully below, the extension of time requested is necessary to fully and completely address the §§ 102 and 103 rejections in the Office Action. The complexity of

the issues raised by the Office Action is exacerbated by (1) the need to investigate the inventive activities behind any and/or all of the rejected claims and the corresponding possibility that at least the Aventail Connect Administrator's Guide ("Aventail"), upon which a § 102(a) rejection is based, is not proper prior art, and (2) the consideration of whether a § 1.132 declaration from a technical expert is appropriate and, importantly, is available under the constraints imposed by the current period for response. Further straining the ability of the Patent Owner to respond to the outstanding rejections are (1) the delay in the Patent Owner's receiving the Office Action after it was mailed, (2) a concurrent trial involving the above-referenced patent, which has caused a significant drain on the Patent Owner's resources, especially the inventors who are necessary to prepare a proper response to the Office Action, and (3) the concurrent reexamination proceedings of a patent related to the above-referenced patent, described below, which has also caused a significant drain on the availability of the Patent Owner's resources. In light of these factors, as more fully explained below, the Patent Owner respectfully requests a two-month extension of time to May 19, 2010 to respond to the outstanding Office Action.

I. Delay in Receipt of The Office Action

Preliminarily, the Patent Owner lost several important and useful days of the period for response. Despite having a mailing date of January 19, 2010, the Office Action was not received by the Patent Owner until January 26, 2010. The Patent Owner filed a Power of Attorney for U.S. Patent No. 7,188,180 ("the '180 patent") on December 15, 2009, which was accepted on December 30, 2009. Because the Patent Owner had not received a Notice of Acceptance, it filed another Power of Attorney on January 14, 2010, before the mailing of the Office Action. This second Power of Attorney was not accepted until January 22, 2010. Despite the Patent Owner's efforts, the Office Action was mailed to its prior patent counsel, who then forwarded the Office Action to the Patent Owner's current counsel on January 25, 2010. For this reason, the Patent Owner did not receive the Office Action until after a critical week of its time period for response expired.

II. Complexity of The Office Action

Preparing a response to the Office Action will involve substantial analysis requiring significant time and resources. Claims 1, 10, 12-15, 17, 26, 28-31, and 33 of the '180 patent are

Petitioner Apple Inc. - Exhibit 1002, p. 332

rejected under 35 U.S.C. §§ 102 and 103 as allegedly being anticipated by and/or rendered obvious by combinations of Aventail, the *VPN: An Overview* reference, the *Network Working Group RFC: 1035* reference, the *Building and Managing Virtual Private Networks* reference by Kosiuer, the *Implementing IPsec* reference by Kaufman, the *Public Key Distribution with Secure DNS* reference by Galvin, the *Gauntlet Firewall for Windows NT Administrator's Guide* reference, the *Windows NT Technical Support: Hands-On* reference, the *Installing, Configuring, and Using PPTP* white paper, and the *Building a Microsoft VPN* reference (collectively "the References"). Preparation of a response to the outstanding Office Action ("the Response") naturally requires substantive analysis of the References and comparison of them to the thirteen rejected claims. The References describe complex systems spanning over 1500 pages. While the Patent Owner has reviewed the References in its due diligence conducted to date, the complexity of each of the References requires a more in depth analysis and comparison by personnel of the Patent Owner, including one or more of the inventors, whose availability within the two month period for response to the Office Action has been and will continue to be limited, as discussed below.

In addition, due to the considerable ramifications of canceling or amending the rejected claims, the Patent Owner believes it necessary to consider providing the Examiner with the views of an independent technical expert in a § 1.132 declaration. To date, the Patent Owner has actively considered the use of and investigated several candidates to serve as a technical expert for providing such a § 1.132 declaration. It has proven extremely difficult to locate such an expert who can provide fully informed views within such a short time-frame – several contacted so far have expressed that there is insufficient time to tackle all of the relevant issues in the time permitted by the current deadline for a response to the Office Action.

The Patent Owner also is necessarily investigating the relevant dates of conception and reduction to practice, as well as diligence therebetween, of the inventions defined in one or more of the rejected claims to determine which of those activities predates the date of publication of one or more of the References, including, for example, Aventail, and, thus, whether or not one or more of the References, including Aventail, constitutes prior art to one or more of the rejected claims. This investigation necessarily requires significant time from the Patent Owner during a time when its relevant personnel, including one or more of the inventors, are strained for time

Petitioner Apple Inc. - Exhibit 1002, p. 333

and attention as a result of their other duties in the co-pending reexamination and the concurrent litigation.

II. Concurrent Litigation and Trial Proceedings

Just at the time when the Patent Owner is in need of significant resources to respond to the Office Action, many of those very resources are now heavily taxed by the pending litigation proceedings involving the '180 patent and others. As mentioned in the Replacement Request for *Inter Partes* Reexamination of Patent, the '180 patent is currently a subject of litigation in Case No. 6:07-cv-80 in the Eastern District of Texas captioned *VirnetX, Inc. v. Microsoft Corp.*, a litigation in which the Requester itself is involved. As provided in the Court's Scheduling Order of June 30, 2009, the jury trial in this litigation is scheduled to begin on March 8, 2010 (following jury selection on March 1, 2010), a mere eleven days before the response to the Office Action is currently due. Various personnel of the Patent Owner are spending significant time in preparing for that trial. As a result, resources and personnel of the Patent Owner required to fully and accurately prepare a response to the Office Action are temporarily limited while the time-consuming trial preparations are conducted as the trial in Texas nears.

While the Patent Owner's counsel continues to perform its due diligence for responding to the Office Action, the looming trial proceedings will make it difficult to complete the Patent Owner's diligence by the current March 19 deadline for response to the Office Action. Moreover, not only would a two month extension permit the resources to be dedicated to responding to this Office Action, it would likely also permit consideration of any court conclusions regarding the claims presently under reexamination.

III. Concurrent Reexamination of Patent No. 6,502,135

Further straining the circumstances are the concurrent *inter partes* reexamination proceedings involving related Patent No. 6,502,135 ("the '135 patent"), which is also at issue in the above-mentioned litigation and is also initiated by the Requester who is involved in litigation. The Office Action mailed January 15, 2010 in the re-examination of the '135 patent ("the Related Reexamination") requires a response due March 15, 2010 – four days before the due date for the response to the Office Action in the present case (a petition for an extension of time is similarly being filed in the Related Reexamination.).

Petitioner Apple Inc. - Exhibit 1002, p. 334

Analyzing the Office Action in preparation for a response in the Related Reexamination has already taken a significant amount of the Patent Owner's resources and personnel, including one or more of the inventors, and will require more of their time in the future. Accordingly, responding to the present Office Action has taken, continues to take, and will continue to take a large amount of the very personnel and resources that are necessary at trial and in the Related Reexamination.

IV. Conclusion

For the reasons stated above, the Patent Owner believes that a two-month extension is appropriate. A prompt decision granting this extension of time is respectfully requested to allow the Patent Owner a fair opportunity to respond to the present Office Action.

Please charge any shortage in fees due in connection with the filing of this paper, including the petition fee of $200.00 set forth in 37 C.F.R. § 1.17(g), to Deposit Account 501133 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

/Toby H. Kusmer/

Toby H. Kusmer, P.C., Reg. No. 26,418
Matthew E. Leno, Reg. No. 41,149
Hasan M. Rashid, Reg. No. 62,390
McDermott Will & Emery LLP
Attorneys for Applicant

28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile: (617)535-3800
tkusmer@mwe.com
mleno@mwe.com
hrashid@mwe.com

Please recognize our Customer No. 23630 as our correspondence address.

Date: February 22, 2010

BST99 1643794-2.077580.0090

Petitioner Apple Inc. - Exhibit 1002, p. 335

Electronic Patent Application Fee Transmittal	
Application Number:	95001270
Filing Date:	08-Dec-2009
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7188180
Filer:	Toby H. Kusmer./Kelly Ciarmataro
Attorney Docket Number:	077580-0090
Filed as Large Entity	

Inter partes reexam Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Petition fee- 37 CFR 1.17(g) (Group II)	1463	1	200	200

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**200**

Electronic Acknowledgement Receipt	
EFS ID:	7061278
Application Number:	95001270
International Application Number:	
Confirmation Number:	2128
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7188180
Customer Number:	23630
Filer:	Toby H. Kusmer./Kelly Ciarmataro
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	077580-0090
Receipt Date:	22-FEB-2010
Filing Date:	08-DEC-2009
Time Stamp:	17:40:23
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$200
RAM confirmation Number	4319
Deposit Account	501133
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Reexam Request for Extension of Time	Petition_Extension_180.pdf	126231 9cc5b30ff77c16dd51a62a1b3c55f1d0b394ddb'	no	5
Warnings:					
Information:					
2	Fee Worksheet (PTO-875)	fee-info.pdf	30504 991e8d9e9d9584340ec76053ad061c49c206453d	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	156735		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Attorney Docket No. 077580-0090

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Reexamination of:	)	
Edmand Munger, et al.	)	
	)	
U.S. Patent No.: 7,188,180	)	
Filed: November 7, 2003	)	**Examiner:**
Issued: March 6, 2007	)	**Andrew L. Nalven**
	)	
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK	)	**Group Art Unit: 3992**
	)	
Reexamination Proceeding	)	
Control No.: 95/001,270	)	
Filed: December 8, 2009	)	

CERTIFICATE OF SERVICE

WE HEREBY CERTIFY that the Petition for Extension of Time Under 37 C.F.R. § 1.956 to Reply to Office Action in Reexamination, filed with United States Patent and Trademark Office on February 22, 2010, was served this 22nd day of February, 2010 on Requester by causing a true copy of same to be deposited as first-class mail for delivery to:

William N. Hughet
Rothwell, Figg, Ernst & Manbeck, P.C.
1425 K Street N.W.
Suite 800
Washington, D.C. 20005

Respectfully submitted,
McDERMOTT WILL & EMERY LLP

Toby H. Kusmer, P.C., Reg. No. 26,418
Matthew E. Leno, Reg. No. 41,149
Hasan M. Rashid, Reg. No. 62,390
McDermott Will & Emery LLP
Attorneys for Applicant
Please recognize our Customer No. 23630 as our correspondence address.

28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile: (617)535-3800
tkusmer@mwe.com,
mleno@mwe.com
hrashid@mwe.com
Date: February 22, 2010

Electronic Acknowledgement Receipt	
EFS ID:	7062751
Application Number:	95001270
International Application Number:	
Confirmation Number:	2128
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7188180
Customer Number:	23630
Filer:	Michael A. Messina/4252/Matilda Mason
Filer Authorized By:	Michael A. Messina
Attorney Docket Number:	077580-0090
Receipt Date:	22-FEB-2010
Filing Date:	08-DEC-2009
Time Stamp:	19:59:44
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Reexam Certificate of Service	077580-0090Certificate.pdf	33031 e3dd6691fdf2d72218676cb546b62b134de a9bb3	no	1

Warnings:
Information:

Total Files Size (in bytes):	33031

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
95/001,270	12/08/2009	7188180	3755-121

CONFIRMATION NO. 2128

23630
MCDERMOTT WILL & EMERY LLP
28 STATE STREET
BOSTON, MA 02109-1775

POA ACCEPTANCE LETTER

OC000000039777323

Date Mailed: 01/22/2010

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 01/14/2010.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/sdstevenson/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Petitioner Apple Inc. - Exhibit 1002, p. 343

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
95/001,270	12/08/2009	7188180	3755-121

CONFIRMATION NO. 2128

POWER OF ATTORNEY NOTICE

22907
BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

Date Mailed: 01/22/2010

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 01/14/2010.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

/sdstevenson/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

REEXAMINATION - PATENT OWNER POWER OF ATTORNEY OR REVOCATION OF POWER OF ATTORNEY WITH A NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS

Control Number(s)	95/001,270
Filing Date(s)	12/08/09
First Named Inventor	Victor Larson
Title	Method for Establishing Secure...
Patent Number	7,188,180
Examiner Name	Lim, Krisna
Attorney Docket No(s).	77580-0090

I hereby revoke all previous patent owner powers of attorney given in the above-identified reexaminaton proceeding control number(s).

☐ A Power of Attorney is submitted herewith.

OR

☒ I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s) to prosecute the proceeding(s) identified above, and to transact all business in the United States Patent and Trademark Office connected therewith: 23630

OR

☐ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) to prosecute the proceeding(s) identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

Practitioner(s) Name	Registration Number

Please recognize or change the correspondence address for the above-identified reexamination proceeding control number(s) (more than one may be changed only if they are merged proceedings) to be:

☒ The address associated with the above-mentioned Customer Number.

OR

☐ The address associated with Customer Number:

OR

☐ Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the:

☐ Inventor, having ownership of the patent being reexamined.

OR

☒ Patent owner.

Statement under 37 CFR 3.73(b) (Form PTO/SB/96) submitted herewith or filed on _____

SIGNATURE of Inventor or Patent Owner

Signature	Victor J. Larson	Date	1/2/2010
Name	Victor J. Larson	Telephone	703-359-4649
Title and Company	R&D Director Virnetx		

NOTE: Signatures of all the inventors or patent owners of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☒ *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/96 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: VirnetX Inc.

Application No./Patent No.: 7,188,180 Filed/Issue Date: 03/06/2007

Titled: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN TWO COMPUTERS OF VIRTUAL PRIVATE NETWORK

VirnetX Inc., a corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.

states that it is:

1. [X] the assignee of the entire right, title, and interest in;

2. [ ] an assignee of less than the entire right, title, and interest in (The extent (by percentage) of its ownership interest is ____ %); or

3. [ ] the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made) the patent application/patent identified above, by virtue of either:

A. [ ] An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel ____, Frame ____, or for which a copy therefore is attached.

OR

B. [X] A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: Larson et al. To: Science Applications International Corp.
The document was recorded in the United States Patent and Trademark Office at Reel 014679, Frame 0947, or for which a copy thereof is attached.

2. From: Science Applications International Corp. To: VirnetX Inc.
The document was recorded in the United States Patent and Trademark Office at Reel 018757, Frame 0328, or for which a copy thereof is attached.

3. From: ____ To: ____
The document was recorded in the United States Patent and Trademark Office at Reel ____, Frame ____, or for which a copy thereof is attached.

[ ] Additional documents in the chain of title are listed on a supplemental sheet(s).

[X] As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (*i.e.*, a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

Signature — Date: 12/15/09

Randall Larsen — Title: President

Printed or Typed Name

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt

EFS ID:	6855360
Application Number:	95001270
International Application Number:	
Confirmation Number:	2128
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7188180
Customer Number:	23630
Filer:	Toby H. Kusmer./Kelly Clarmataro
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	3755-121
Receipt Date:	21-JAN-2010
Filing Date:	08-DEC-2009
Time Stamp:	15:40:56
Application Type:	Inter partes reexam

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	ReexamPOA.pdf	67354 978fe33d73fbad05100755 9e599897ecffc6	no	1

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
2	Assignee showing of ownership per 37 CFR 3.73(b).	Larson_Statement.pdf	743249 d7d8549a8d0fd27801e95429654a26a3cf6497fd	no	1
Warnings:					
Information:					
			Total Files Size (in bytes):	810603	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

REEXAMINATION - PATENT OWNER POWER OF ATTORNEY OR REVOCATION OF POWER OF ATTORNEY WITH A NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS

Control Number(s)	95/001,270
Filing Date(s)	12/08/09
First Named Inventor	Victor Larson
Title	Method for Establishing Secure...
Patent Number	7,188,180
Examiner Name	Lim, Krisna
Attorney Docket No(s).	77580-0090

I hereby revoke all previous patent owner powers of attorney given in the above-identified reexamination proceeding control number(s).

☐ A Power of Attorney is submitted herewith.

OR

☒ I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s) to prosecute the proceeding(s) identified above, and to transact all business in the United States Patent and Trademark Office connected therewith: 23630

OR

☐ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) to prosecute the proceeding(s) identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

Practitioner(s) Name	Registration Number

Please recognize or change the correspondence address for the above-identified reexamination proceeding control number(s) (more than one may be changed only if they are merged proceedings) to be:

☒ The address associated with the above-mentioned Customer Number.

OR

☐ The address associated with Customer Number:

OR

☐ Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the:

☐ Inventor, having ownership of the patent being reexamined.

OR

☒ Patent owner.

Statement under 37 CFR 3.73(b) (Form PTO/SB/96) submitted herewith or filed on _____.

SIGNATURE of Inventor or Patent Owner

Signature	Victor J. Larson	Date	1/2/2010
Name	Victor J. Larson	Telephone	703-359-4649
Title and Company	R&D Director Virnetx		

NOTE: Signatures of all the inventors or patent owners of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*

☒ *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Bib Data Sheet

CONFIRMATION NO. 2128

SERIAL NUMBER	FILING OR 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
95/001,270	12/08/2009 RULE	709	3992	3755-121

APPLICANTS

7188180, Residence Not Provided;
VIRNETX INC.(OWNER), SCOTTSVALLEY DRIVE, CA;
MICROSOFT CORPORATION(3RD. PTY. REQ.), CHEVY CHASE, MD;
MICROSOFT CORPORATION(REAL PTY. IN INTEREST), CHEVY CHASE, MD;
ROTHWELL, FIGG, ERNST & MANBECK, P.C., WASHINGTON, DC

**** CONTINUING DATA ***************************

This application is a REX of 10/702,486 11/07/2003 PAT 7,188,180
which is a DIV of 09/558,209 04/26/2000 ABN
which is a CIP of 09/504,783 02/15/2000 PAT 6,502,135
which is a CIP of 09/429,643 10/29/1999 PAT 7,010,604
which claims benefit of 60/106,261 10/30/1998
and claims benefit of 60/137,704 06/07/1999

**** FOREIGN APPLICATIONS *********************

Foreign Priority claimed	STATE OR COUNTRY	SHEETS DRAWING	TOTAL CLAIMS	INDEPENDENT CLAIMS
☐ yes ☐ no				
35 USC 119 (a-d) conditions met ☐ yes ☐ no ☐ Met after Allowance				
Verified and Acknowledged Examiner's Signature Initials				

ADDRESS
23630

TITLE
METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

FILING FEE RECEIVED	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/001,270	12/08/2009	7188180	3755-121	2128

22907 7590 01/19/2010
BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

EXAMINER	
NALVEN, ANDREW L	
ART UNIT	**PAPER NUMBER**
3992	

MAIL DATE	DELIVERY MODE
01/19/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patents and Trademark Office
P.O.Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

MAILED

Date: JAN 19 2010

CENTRAL REEXAMINATION UNIT

THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS
ROTHWELL, FIGG, ERNST & MANBECK, P.C.
1425 K STREET N.W.
SUITE 800
WASHINGTON, D.C. 20005

Transmittal of Communication to Third Party Requester
Inter Partes Reexamination

REEXAMINATION CONTROL NO. : 95001270
PATENT NO. : 7188180
TECHNOLOGY CENTER : 3999
ART UNIT : 3992

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified Reexamination proceeding. 37 CFR 1.903.

Prior to the filing of a Notice of Appeal, each time the patent owner responds to this communication, the third party requester of the inter partes reexamination may once file written comments within a period of 30 days from the date of service of the patent owner's response. This 30-day time period is statutory (35 U.S.C. 314(b)(2)), and, as such, it cannot be extended. See also 37 CFR 1.947.

If an ex parte reexamination has been merged with the inter partes reexamination, no responsive submission by any ex parte third party requester is permitted.

All correspondence relating to this inter partes reexamination proceeding should be directed to the Central Reexamination Unit at the mail, FAX, or hand-carry addresses given at the end of the communication enclosed with this transmittal.

PTOL-2070(Rev.07-04)

ORDER GRANTING/DENYING REQUEST FOR* INTER PARTES *REEXAMINATION	**Control No.**	**Patent Under Reexamination**	
	95/001,270	7188180	
	Examiner	**Art Unit**	
	ANDREW L. NALVEN	3992	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

The request for *inter partes* reexamination has been considered. Identification of the claims, the references relied on, and the rationale supporting the determination are attached.

Attachment(s): ☐ PTO-892 ☒ PTO/SB/08 ☒Other: Decision on Request

1. ☒ The request for *inter partes* reexamination is GRANTED.

☒ An Office action is attached with this order.

☐ An Office action will follow in due course.

2. ☐ The request for *inter partes* reexamination is DENIED.

This decision is not appealable. 35 U.S.C. 312(c). Requester may seek review of a denial by petition to the Director of the USPTO within ONE MONTH from the mailing date hereof. 37 CFR 1.927. EXTENSIONS OF TIME ONLY UNDER 37 CFR 1.183. In due course, a refund under 37 CFR 1.26(c) will be made to requester.

All correspondence relating to this *inter partes* reexamination proceeding should be directed to the **Central Reexamination Unit** at the mail, FAX, or hand-carry addresses given at the end of this Order.

DECISION GRANTING INTER PARTES REEXAMINATION

A substantial new question of patentability affecting claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of United States Patent Number 7,188,180 (hereafter "the '180 patent") is raised by the request for *inter partes* reexamination submitted on December 8, 2009.

Notification of Concurrent Proceedings

The patent owner is reminded of the continuing responsibility under 37 CFR 1.985 to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving the '180 patent throughout the course of this reexamination proceeding. The third party requester is also reminded of the ability to similarly apprise the Office of any such activity or proceeding throughout the course of this reexamination proceeding. See MPEP § 2686 and 2686.04.

PROSECUTION HISTORY

The '180 patent was issued on March 6, 2007 from an application filed November 7, 2003. During the prosecution of the '180 patent, a notice of allowance was issued on November 12, 2006. The notice of allowance specified the reasons for allowance as the failure of the prior art to teach "requesting a secure computer network address from

a secure domain name server according to the secure domain name; and using a virtual private network communication link to send an access request message to the secure computer network address" (see prosecution history of application 10/702,486, Notice of Allowance mailed 11/12/2006).

PROPOSED SUBSTANTIAL NEW QUESTIONS OF PATENTABILITY

Third Party Requester ("Requester") requested reexamination of claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of the '180 patent based upon the following prior art patents and publications:

1. Aventail Administrator's Guide (hereafter "Aventail") that was published between 1996 and 1999. Aventail was not considered in a prior examination and qualifies as prior art under §102(a).
2. Microsoft Windows NT Server, Virtual Private Networking: An Overview (hereafter "VPN Overview") that was published in 1998. VPN Overview was not considered in a prior examination and qualifies as prior art under §102(b).
3. RFC 1035 that was published in 1987. RFC 1035 was not considered in a prior examination and qualifies as prior art under §102(b).
4. "Building and Managing Virtual Private Networks" that was published by David Kosiur in 1998 (hereafter "Kosiur"). Kosiur was not considered in a prior examination and qualifies as prior art under §102(b).

5. "Implementing IPsec" that was published by Elizabeth Kaufman on September 7, 1999 (hereafter "Kaufman." Kaufman was not considered in a prior examination and qualifies as prior art under §102(a).
6. "Public Key Distribution with Secure DNS" by James Galvin that was published in July 1996 (hereafter "Galvin"). Galvin was not considered during a prior examination and qualifies as prior art under §102(b).
7. Gauntlet Firewall for Windows NT, Administrator's Guide (hereafter "Gauntlet") that was published no later than 1999. Gauntlet was not considered in a prior examination and qualifies as prior art under §102(a).
8. Microsoft Windows NT Technical Support: Hands-On, Self-paced Training for Support Version 4.0 (hereafter "Hands-On"). Hands-On was published in 1998 and qualifies as prior art under §102(b). Hands-On was not considered in a prior examination.
9. Microsoft Windows NT Sever, Whitepaper: Installing, Configuring, and Using PPTP with Microsoft Clients and Severs (hereafter "Installing NT"). Installing NT was published in 1997 and qualifies as prior art under §102(b). Installing NT was not considered in a prior examination.
10. Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources (hereafter "Microsoft VPN") that was published on January 1, 2000. Microsoft VPN was not considered in a prior examination and qualifies as prior art under §102(a).

Requestor has alleged a substantial new question of patentability in light of the proposed rejections:

Issue 1 - Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are anticipated by Aventail under 35 U.S.C. §102(a).

Issue 2 - Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are rendered obvious by the combination of VPN Overview in view of RFC 1035 under 35 U.S.C. 103(a).

Issue 3 - Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are anticipated by Kosiur under 35 U.S.C. §102(b).

Issue 4 - Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are anticipated by Kaufman under 35 U.S.C. §102(a).

Issue 5 - Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are rendered obvious by the combination of Kaufman in view of Galvin under 35 U.S.C. 103(a).

Issue 6 - Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are anticipated by Gauntlet under 35 U.S.C. §102(a).

Issue 7 - Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are rendered obvious by the combination of Hands-On in view of Installing NT under 35 U.S.C. 103(a).

Issue 8 - Claims 1, 10, 12-15, 17, 26, 28-31, and 33 are anticipated by Microsoft VPN under 35 U.S.C. §102(a).

ANALYSIS OF SUBSTANTIAL NEW QUESTIONS OF PATENTABILITY

Summary

Requestor has shown a substantial new question of patentability with regards to claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35.

Analysis

A substantial new question of patentability is raised by a cited patent or printed publication when there is a substantial likelihood that a reasonable examiner would consider the prior art patent or printed publication important in deciding whether or not the claim is patentable. A substantial new question of patentability is not raised by prior art presented in a reexamination request if the Office has previously considered (in an earlier examination of the patent) the same question of patentability as to a patent claim favorable to the patent owner based on the same prior art patents or printed publications. In re Recreative Technologies, 83 F.3d 1394, 38 USPQ2d 1776 (Fed. Cir. 1996).

Aventail Reference

Aventail raises a substantial new question of patentability regarding claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 as presented in Issue 1. Aventail raises a substantial new question by providing teachings that were not considered in a previous examination and that are relevant to the designated allowable subject matter.

For example, Aventail at least discloses requesting a secure computer network address from a secure domain name server according to the secure domain name (Aventail, page 11, the application does a DNS lookup). Aventail's DNS request seeks a "secure" computer network address because Aventail discloses the listing of domain names associated with a redirection rule. These special domains require the proxying of traffic (Aventail, page 11). When proxying the traffic to the secure computer network address, Aventail executes authentication processing (Aventail, page 11) and in some cases transmits and receives data using encryption (Aventail, page 12).

These teachings would be important to a reasonable examiner in deciding patentability because the prosecution history suggests that these features were the reason for allowance of the claims. Thus, there is a substantial likelihood that a reasonable examiner would consider Aventail important in deciding whether or not the claims are patentable. Accordingly, Aventail raises a substantial new question of patentability as to claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 that has not been decided in a previous examination.

VPN Overview Reference

VPN Overview raises a substantial new question of patentability regarding claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 as presented in Issue 2. VPN Overview raises a substantial new question by providing teachings that were not considered in a previous examination and that are relevant to the designated allowable subject matter.

For example, VPN Overview at least discloses sending an access request message to the secure computer network address using a virtual private network communication link (VPN Overview, page 9 – gain access to the protected resources). VPN Overview discloses an access request message by disclosing that a client gains access to protected resources of a corporate hub (VPN Overview, page 9). This necessarily implies that the client is requesting access to some particular resource. The requests for access are transmitted through the established VPN in order to ensure that only those users with proper credentials can gain access to the protected resources.

These teachings would be important to a reasonable examiner in deciding patentability because the prosecution history suggests that these features were the reason for allowance of the claims. Thus, there is a substantial likelihood that a reasonable examiner would consider VPN Overview important in deciding whether or not the claims are patentable. Accordingly, VPN Overview raises a substantial new question of patentability as to claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 that has not been decided in a previous examination.

Kosiur Reference

Kosiur raises a substantial new question of patentability regarding claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 as presented in Issue 3. Kosiur raises a substantial new question by providing teachings that were not considered in a previous examination and that are relevant to the designated allowable subject matter.

For example, Kosiur at least discloses sending an access request message to the secure computer network address using a virtual private network communication link (Kosiur, pages 40-42). Kosiur discloses this limitation, a basis for allowance of the '180 patent, by teaching the use of the VPN to access information over a network connection. By accessing information over a VPN, Kosiur requires the sending of an access request message.

These teachings would be important to a reasonable examiner in deciding patentability because the prosecution history suggests that these features were the reason for allowance of the claims. Thus, there is a substantial likelihood that a reasonable examiner would consider Kosiur important in deciding whether or not the claims are patentable. Accordingly, Kosiur raises a substantial new question of patentability as to claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 that has not been decided in a previous examination.

Kaufman Reference

Kaufman raises a substantial new question of patentability regarding claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 as presented in Issues 4 and 5. Kaufman raises a substantial new question by providing teachings that were not considered in a previous examination and that are relevant to the designated allowable subject matter.

For example, Kaufman at least discloses sending an access request message to the secure computer network address using a virtual private network communication link (Kaufman, Pages 65, 94, and 141). Kaufman discloses the limitation by teaching

that a VPN connection is used to securely connect to a remote device in order to access content (Kaufman, Pages 65 and 141).

These teachings would be important to a reasonable examiner in deciding patentability because the prosecution history suggests that these features were the reason for allowance of the claims. Thus, there is a substantial likelihood that a reasonable examiner would consider Kaufman important in deciding whether or not the claims are patentable. Accordingly, Kaufman raises a substantial new question of patentability as to claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 that has not been decided in a previous examination.

Gauntlet Reference

Gauntlet raises a substantial new question of patentability regarding claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 as presented in Issue 6. Gauntlet raises a substantial new question by providing teachings that were not considered in a previous examination and that are relevant to the designated allowable subject matter.

For example, Gauntlet at least discloses sending an access request message to the secure computer network address using a virtual private network communication link (Gauntlet, Section 18-1, client can connect through PPTP to read mail or access other internal data). Gauntlet discloses this limitation, a basis for allowance of the '180 patent, by teaching the use of the VPN to access information over a network connection which suggests that there must be a request for information.

These teachings would be important to a reasonable examiner in deciding patentability because the prosecution history suggests that these features were the reason for allowance of the claims. Thus, there is a substantial likelihood that a reasonable examiner would consider Gauntlet important in deciding whether or not the claims are patentable. Accordingly, Gauntlet raises a substantial new question of patentability as to claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 that has not been decided in a previous examination.

Hands-On Reference

Hands-On raises a substantial new question of patentability regarding claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 as presented in Issue 7. Hands-On raises a substantial new question by providing teachings that were not considered in a previous examination and that are relevant to the designated allowable subject matter.

For example, Hands-On at least discloses sending an access request message to the secure computer network address using a virtual private network communication link (Hands-On, Page 431, remotely access corporate network). Hands-On discloses this limitation, a basis for allowance of the '180 patent, by teaching the use of the VPN to access information over a network connection which suggests that there must be a request for information.

These teachings would be important to a reasonable examiner in deciding patentability because the prosecution history suggests that these features were the reason for allowance of the claims. Thus, there is a substantial likelihood that a

reasonable examiner would consider Hands-On important in deciding whether or not the claims are patentable. Accordingly, Hands-On raises a substantial new question of patentability as to claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 that has not been decided in a previous examination.

Microsoft VPN Reference

Microsoft VPN raises a substantial new question of patentability regarding claims 1, 4, 10, 12-15, 17, 20, 26, and 28-31 as presented in Issue 8. Microsoft VPN raises a substantial new question by providing teachings that were not considered in a previous examination and that are relevant to the designated allowable subject matter.

For example, Microsoft VPN at least discloses sending an access request message to the secure computer network address using a virtual private network communication link (Microsoft VPN, Pages 11-12, remote access to an organization server). Microsoft VPN discloses this limitation, a basis for allowance of the '180 patent, by teaching the use of the VPN to access information over a network connection which suggests that there must be a request for information.

These teachings would be important to a reasonable examiner in deciding patentability because the prosecution history suggests that these features were the reason for allowance of the claims. Thus, there is a substantial likelihood that a reasonable examiner would consider Microsoft VPN important in deciding whether or not the claims are patentable. Accordingly, Microsoft VPN raises a substantial new

question of patentability as to claims 1, 4, 10, 12-15, 17, 20, 26, and 28-31 that has not been decided in a previous examination.

CORRESPONDENCE

All correspondence relating to this inter partes reexamination proceeding should be directed:

By EFS: Registered users may submit via the electronic filing system EFS-Web, at https://sportal.uspto.gov/authenticate/authenticateuserlocalepf.html.

By Mail to:
Mail Stop *Inter Partes* Reexam
Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to:
(571) 273-9900
Central Reexamination Unit

By hand:
Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

For EFS-Web transmissions, 37 CFR 1.8(a)(1)(i) (C) and (ii) states that correspondence (except for a request for reexamination and a corrected or replacement request for reexamination) will be considered timely filed if (a) it is transmitted via the Office's electronic filing system in accordance with 37 CFR 1.6(a)(4), and (b) includes a

certificate of transmission for each piece of correspondence stating the date of transmission, which is prior to the expiration of the set period of time in the Office action.

Any inquiry concerning this communication or earlier communications from the Examiner, or as to the status of this proceeding, should be directed to the Central Reexamination Unit at telephone number (571) 272-7705.

Signed:

/Andrew Nalven/

Andrew Nalven
CRU Examiner
GAU 3992
(571) 272-3839

Conferee: ESK

Conferee: AJK

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/001,270	12/08/2009	7188180	3755-121	2128

22907 7590 01/19/2010
BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

EXAMINER	
NALVEN, ANDREW L.	

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
01/19/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

OFFICE ACTION IN INTER PARTES REEXAMINATION	Control No. 95/001,270	Patent Under Reexamination 7188180	
	Examiner ANDREW L. NALVEN	Art Unit 3992	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

Responsive to the communication(s) filed by:
Patent Owner on _____
Third Party(ies) on 8 December 2009

RESPONSE TIMES ARE SET TO EXPIRE AS FOLLOWS:

For Patent Owner's Response:
2 MONTH(S) from the mailing date of this action. 37 CFR 1.945. EXTENSIONS OF TIME ARE GOVERNED BY 37 CFR 1.956.
For Third Party Requester's Comments on the Patent Owner Response:
30 DAYS from the date of service of any patent owner's response. 37 CFR 1.947. NO EXTENSIONS OF TIME ARE PERMITTED. 35 U.S.C. 314(b)(2).

All correspondence relating to this inter partes reexamination proceeding should be directed to the **Central Reexamination Unit** at the mail, FAX, or hand-carry addresses given at the end of this Office action.

This action is not an Action Closing Prosecution under 37 CFR 1.949, nor is it a Right of Appeal Notice under 37 CFR 1.953.

PART I. THE FOLLOWING ATTACHMENT(S) ARE PART OF THIS ACTION:

1. ☐ Notice of References Cited by Examiner, PTO-892
2. ☒ Information Disclosure Citation, PTO/SB/08
3. ☐ _____

PART II. SUMMARY OF ACTION:

1a. ☒ Claims 1,4,10,12-15,17,20,26,28-31,33 and 35 are subject to reexamination.
1b. ☒ Claims 2, 3, 5-9, 11, 16, 18,19, 21-25, 27, 32, 34, 36-41 are not subject to reexamination.
2. ☐ Claims _____ have been canceled.
3. ☒ Claims 4,20,35 are confirmed. [Unamended patent claims] ESL
4. ☐ Claims _____ are patentable. [Amended or new claims]
5. ☒ Claims 1, 10,12-15,17,26,28-31,33 are rejected.
6. ☒ Claims ~~4,20 and 35~~ are objected to. ESL
7. ☐ The drawings filed on _____ ☐ are acceptable ☐ are not acceptable.
8. ☐ The drawing correction request filed on _____ is: ☐ approved. ☐ disapproved.
9. ☐ Acknowledgment is made of the claim for priority under 35 U.S.C. 119 (a)-(d). The certified copy has: ☐ been received. ☐ not been received. ☐ been filed in Application/Control No ~~95001270~~.
10. ☐ Other _____

Inter Partes Reexamination Office Action

Third Party Requester ("Requester") requested reexamination of claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of United States Patent Number 7,188,180 (hereafter "the '180 patent") issued to Larson et al based upon the following prior art patents and publications:

1. Aventail Administrator's Guide (hereafter "Aventail") that was published between 1996 and 1999. Aventail was not considered in a prior examination and qualifies as prior art under §102(a).
2. Microsoft Windows NT Server, Virtual Private Networking: An Overview (hereafter "VPN Overview") that was published in 1998. VPN Overview was not considered in a prior examination and qualifies as prior art under §102(b).
3. RFC 1035 that was published in 1987. RFC 1035 was not considered in a prior examination and qualifies as prior art under §102(b).
4. "Building and Managing Virtual Private Networks" that was published by David Kosiur in 1998 (hereafter "Kosiur"). Kosiur was not considered in a prior examination and qualifies as prior art under §102(b).
5. "Implementing IPsec" that was published by Elizabeth Kaufman on September 7, 1999 (hereafter "Kaufman." Kaufman was not considered in a prior examination and qualifies as prior art under §102(a).

6. "Public Key Distribution with Secure DNS" by James Galvin that was published in July 1996 (hereafter "Galvin"). Galvin was not considered during a prior examination and qualifies as prior art under §102(b).
7. Gauntlet Firewall for Windows NT, Administrator's Guide (hereafter "Gauntlet") that was published no later than 1999. Gauntlet was not considered in a prior examination and qualifies as prior art under §102(a).
8. Microsoft Windows NT Technical Support: Hands-On, Self-paced Training for Support Version 4.0 (hereafter "Hands-On"). Hands-On was published in 1998 and qualifies as prior art under §102(b). Hands-On was not considered in a prior examination.
9. Microsoft Windows NT Sever, Whitepaper: Installing, Configuring, and Using PPTP with Microsoft Clients and Severs (hereafter "Installing NT"). Installing NT was published in 1997 and qualifies as prior art under §102(b). Installing NT was not considered in a prior examination.
10. Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources (hereafter "Microsoft VPN") that was published on January 1, 2000. Microsoft VPN was not considered in a prior examination and qualifies as prior art under §102(a).

The attached order granting reexamination found a substantial new question of patentability raised by the following proposed rejections:

Issue 1 - Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are anticipated by Aventail under 35 U.S.C. §102(a).

Issue 2 - Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are rendered obvious by the combination of VPN Overview in view of RFC 1035 under 35 U.S.C. 103(a).

Issue 3 - Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are anticipated by Kosiur under 35 U.S.C. §102(b).

Issue 4 - Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are anticipated by Kaufman under 35 U.S.C. §102(a).

Issue 5 - Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are rendered obvious by the combination of Kaufman in view of Galvin under 35 U.S.C. 103(a).

Issue 6 - Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are anticipated by Gauntlet under 35 U.S.C. §102(a).

Issue 7 - Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are rendered obvious by the combination of Hands-On in view of Installing NT under 35 U.S.C. 103(a).

Issue 8 - Claims 1, 10, 12-15, 17, 26, 28-31, and 33 are anticipated by Microsoft VPN under 35 U.S.C. §102(a).

Claim Rejections - 35 USC § 102 and 103

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Issue 1

Requester proposed rejections of Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 as anticipated by Aventail under 35 U.S.C. §102(a). These proposed rejections are adopted in part.

Claims 1, 10, 12, 14, 17, 26, 28, 30, 31, and 33 are rejected under 35 U.S.C. 102(a) as being anticipated by Aventail. This rejection for claims 1, 1, 10, 12, 14, 17, 26, 28, 30, 31, and 33 is adopted for the reasons set forth in the December 8,

2009 request for reexamination, on pages 12-19 and as presented in Appendix A, which is incorporated by reference. In addition, a rejection of claims 1, 10, 12, 14, 17, 26, 28, 30, 31, and 33 in view of Aventail is provided below which utilizes citations to Aventail provided in the request and additional citations provided by Examiner.

With regards to claim 1, Aventail teaches a method for accessing a secure computer network address (*Aventail, Page 11 – Application does a DNS lookup to convert hostname into IP network address; Page 46 - SOCKS v5 servers often require user authentication before allowing access; Page 66 – To gain access to your extranet, users may need to traverse multiple firewalls...employee at a partner company...having an authenticated, encrypted, and controlled connection to your internal network*),

comprising steps of: receiving a secure domain name (*Aventail, Page 11 – Application does a DNS lookup to convert hostname into IP network address; Pages 12-13 – if the requested domain name matches a redirection rule then it is part of a domain we are proxying traffic to – the domain name is secure because this traffic is routed through a SOCKS server and utilizes authentication methods and in some cases encryption; Examiner is interpreting the secure domain name as a domain name associated with a secure computer*);

sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name (*Aventail, Page 12 - "If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a False DNS entry (HOSTENT) that it*

can recognize during the connection request. Aventail Connect will forward the hostname to the extranet SOCKS server in step 2 and the SOCKS server performs the hostname resolution," the SOCKS server acts to resolve/request the secure computer network address from a secure domain name service; Examiner is interpreting the query message as a DNS resolution request to a domain name server that can resolve addresses of secure computers);

receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name (*Aventail, Page 12 – "If the destination hostname matches a redirection rule...Aventail Connect will forward the hostname to the extranet SOCKS server and the SOCKS server performs the hostname resolution." Since the SOCKS server performs hostname resolution by requesting the secure computer network address, it is inherent that a message should be received that resolves the domain name to an address; Examiner is interpreting the response message as a DNS resolution message returning an address associated with a secure computer*);

and sending an access request message to the secure computer network address using a virtual private network communication link (*Aventail, Page 77 – "The Aventail ExtraNet depicted in this example is used to provide secure and monitored access to the private LAN for mobile employees and partners." – Users access the remote network through a VPN and request access to resources/content of the remote network through the VPN; Examiner is interpreting the sending of the access request message as requesting access to a particular resource/content over a VPN*).

With regards to claim 10, Aventail teaches the virtual private network includes the Internet (*Aventail, Page 5 – "Aventail...extranet solutions allow organizations to secure their networked communications and manage their employees' access to the Internet. Building an extranet gives organizations the ability to dynamically create a private communication or data channel over the Internet"*).

With regards to claim 12, Aventail teaches the access request message contains a request for information stored at the secure computer network address (*Aventail, Page 77 – "The Aventail ExtraNet depicted in this example is used to provide secure and monitored access to the private LAN for mobile employees and partners." – Users access the remote network through a VPN and request access to resources/content of the remote network through the VPN*).

With regards to claim 14, Aventail teaches the method of claim 1 performed by a software module (*Aventail, Page 7 – Aventail Connect is a client component. Aventail ExtraNet Server is a component that runs on a SOCKS 5 server; Page 9 – Aventail Connect is a layered service provider*).

With regards to claim 17, Aventail teaches a computer-readable storage medium, comprising: a storage area *(Aventail, Page 14 - Aventail Connect can be delivered on CD or as a network- delivered, self-extracting archive file; Page 15 - Aventail Connect can be installed to single workstation or to multiple networked workstations)*;

and computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of: receiving a secure domain

name (*Aventail, Page 11 – Application does a DNS lookup to convert hostname into IP network address; Pages 12-13 – if the requested domain name matches a redirection rule then it is part of a domain we are proxying traffic to – the domain name is secure because this traffic is routed through a SOCKS server and utilizes authentication methods and in some cases encryption)*;

sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain name (*Aventail, Page 12 - "If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a False DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet SOCKS server in step 2 and the SOCKS server performs the hostname resolution," the SOCKS server acts to resolve/request the secure computer network address from a secure domain name service)*;

receiving from the domain name service a response message containing the secure computer network address corresponding to the secure domain name (*Aventail, Page 12 – "If the destination hostname matches a redirection rule...Aventail Connect will forward the hostname to the extranet SOCKS server and the SOCKS server performs the hostname resolution." Since the SOCKS server performs hostname resolution by requesting the secure computer network address, it is inherent that a message should be received that resolves the domain name to an address)*;

and sending an access request message to the secure computer network address using a virtual private network communication link (*Aventail, Page 77 – "The Aventail ExtraNet depicted in this example is used to provide secure and monitored access to the private LAN for mobile employees and partners." – Users access the remote network through a VPN and request access to resources/content of the remote network through the VPN).*

With regards to claim 26, Aventail teaches the virtual private network includes the Internet (*Aventail, Page 5 – "Aventail...extranet solutions allow organizations to secure their networked communications and manage their employees' access to the Internet. Building an extranet gives organizations the ability to dynamically create a private communication or data channel over the Internet"*).

With regards to claim 28, Aventail teaches the access request message contains a request for information stored at the secure computer network address (*Aventail, Page 77 – "The Aventail ExtraNet depicted in this example is used to provide secure and monitored access to the private LAN for mobile employees and partners." – Users access the remote network through a VPN and request access to resources/content of the remote network through the VPN*).

With regards to claim 30, Aventail teaches the method of claim 1 performed by a software module (*Aventail, Page 7 – Aventail Connect is a client component. Aventail ExtraNet Server is a component that runs on a SOCKS 5 server; Page 9 – Aventail Connect is a layered service provider*).

With regards to claim 33, Aventail teaches a data processing apparatus, comprising: a processor, and memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address (*Aventail, Page 14 - Aventail Connect can be delivered on CD or as a network- delivered, self-extracting archive file; Page 15 - Aventail Connect can be installed to single workstation or to multiple networked workstations)*,

said method comprising steps of: receiving a secure domain name (*Aventail, Page 11 – Application does a DNS lookup to convert hostname into IP network address; Pages 12-13 – if the requested domain name matches a redirection rule then it is part of a domain we are proxying traffic to – the domain name is secure because this traffic is routed through a SOCKS server and utilizes authentication methods and in some cases encryption)*;

sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name (*Aventail, Page 12 - "If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a False DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet SOCKS server in step 2 and the SOCKS server performs the hostname resolution," the SOCKS server acts to resolve/request the secure computer network address from a secure domain name service)*;

receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name (*Aventail, Page 12 – "If the destination hostname matches a redirection rule...Aventail Connect will forward the hostname to the extranet SOCKS server and the SOCKS server performs the hostname resolution." Since the SOCKS server performs hostname resolution by requesting the secure computer network address, it is inherent that a message should be received that resolves the domain name to an address)*;

and sending an access request message to the secure computer network address using a virtual private network communication link (*Aventail, Page 77 – "The Aventail ExtraNet depicted in this example is used to provide secure and monitored access to the private LAN for mobile employees and partners." – Users access the remote network through a VPN and request access to resources/content of the remote network through the VPN).*

The rejection of claims 4, 13, 15, 20, 29, 31, and 35 as anticipated by Aventail, as proposed in the request, is not adopted for the following reasons.

Claims 4, 20, and 35.

Claims 4, 20, and 35 further limit their parent claims by requiring that the response message contain provisioning information for the virtual private network. The response message is defined in claim 1 as "containing the secure computer network address corresponding to the secure domain name" that is received in response to a

"query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name." In other words, a query message requests a secure computer network address corresponding to a secure domain name and a response message is received that includes both (1) the secure computer network address and (2) provisioning information for the virtual private network.

Aventail fails to teach the response message containing provisioning information for the virtual private network in addition to the secure computer network address as described above. Aventail does teach that a query message is sent to request a secure computer network address corresponding to a secure domain name (*Aventail, Page 12 –SOCKS server performs the hostname resolution*). Aventail further inherently teaches that a response message returns the secure network address because DNS resolution returns an address that corresponds to a domain name. However, Aventail does not teach that the response message includes not only the secure network address, but also VPN provisioning information.

Claims 13, 15, 29, and 31.

Claims 13 and 29 further limit their parent claims by requiring "receiving the secure domain name comprises receiving the secure domain name at a client computer from a user; wherein sending the query message comprises sending the query message at the client computer; wherein receiving the response message comprises receiving the response message at the client computer, wherein sending the access

request message comprises sending the access request message at the client computer." Aventail fails to teach each and every limitation and thus fails to anticipate claims 13 and 29.

Aventail teaches receiving the secure domain name comprises receiving the secure domain name at a client computer from a user (*Aventail, Page 8 – the application executes a DNS lookup. The application is run by the user at the client*);

wherein sending the query message comprises sending the query message at the client computer (*Aventail, Page 8 – the application executes a DNS lookup. The application is run on the client and thus the query message is sent at the client)*;

wherein sending the access request message comprises sending the access request message at the client computer (*Aventail, Page 77 – "The Aventail ExtraNet depicted in this example is used to provide secure and monitored access to the private LAN for mobile employees and partners." – Users access the remote network through a VPN and request access to resources/content of the remote network through the VPN).*

However, Aventail fails to teach receiving the response message at the client computer. The response message is defined in claim 1 as "containing the secure computer network address corresponding to the secure domain name" that is received in response to a "query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name." Aventail fails to disclose the response message including a secure computer network address being received by the client. Instead, Aventail discloses that response messages including non-secure computer network addresses are received by the client

(*Aventail, Page 11 – if the hostname matches a local domain string or does not match a redirection rule...performs lookup as if Aventail Connect were not running. Thus the DNS resolution response message would be returned to the client*).

Aventail discloses that in the case of a request for a secure computer network address, the secure computer network address is not returned to the client (*Aventail, Page 12 – the request is for a secure computer network address when the destination hostname matches a redirection rule*). Instead, a false DNS entry is returned in a response message to the client (*Aventail, Page 12 - HOSTENT*). Thus, Aventail fails to disclose a response message being received at the client computer that includes the secure computer network address as required by claim 13.

For reasons similar to those as above, Aventail fails to anticipate claim 15 and 31's limitation requiring the method to be being performed by the client computer. As noted above, in the case of a request for a secure computer network address, Aventail fails to disclose a response message being received at the client computer that includes the secure computer network address. Thus, Aventail fails to teach "the method" being performed by the client computer.

Issue 2

Requester proposed rejections of Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 as rendered obvious by the combination of VPN Overview in view of RFC 1035 under 35 U.S.C. 103(a). These proposed rejections are adopted in part.

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over VPN Overview in view of RFC 1035.

This rejection for claims 1, 10, 12-15, 17, 26, 28-31, and 33 is adopted for the reasons set forth in the December 8, 2009 request for reexamination which is incorporated by reference (*see Request for Reexamination, pages 19-25 and Appendix B).*

The rejection of claims 4, 20, and 35 as unpatentable over VPN Overview in view of RFC 1035, as proposed in the request, is not adopted for the following reasons.

Claims 4, 20, and 35.

Claims 4, 20, and 35 further limit their parent claims by requiring that the response message contain provisioning information for the virtual private network. The response message is defined in claim 1 as "containing the secure computer network address corresponding to the secure domain name" that is received in response to a "query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name." In other words, a query message requests a secure computer network address corresponding to a secure domain name and a response message is received that includes both (1) the secure computer network address and (2) provisioning information for the virtual private network.

Both VPN Overview and RFC 1035 fail to teach a response message containing provisioning information for the virtual private network in addition to the secure computer network address as described above. VPN Overview teaches connection requests that result in the creation of VPN connections (*VPN Overview, Page 22 – compulsory tunneling create after initial connection is made*). In teaching VPN connections, VPN Overview's disclosures inherently teach that provisioning information is received by the client computer (*see VPN Overview, Pages 9,,26, and 27*). However, VPN Overview fails to specifically disclose the provisioning information because sent in a response message to a DNS query message.

Further, RFC 1035 fails to teach a response message containing provisioning information for the virtual private network. RFC 1035 discloses the standard for domain name resolution of Internet domain names (*RFC 1035, Page 4*). RFC 1035 discloses that in response to a user query for the resolution of a domain name; a response is received that includes the domain name address (*RFC 1035, Page 4, User responses*). However, RFC 1035's response message fails to include VPN provisioning information. Thus, Both VPN Overview and RFC 1035 fail to teach a response message containing provisioning information for the virtual private network in addition to the secure computer network address as described above.

Issue 3

Requester proposed rejections of Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 as anticipated by Kosiur under 35 U.S.C. §102(b). These proposed rejections are adopted in part.

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 are rejected under 35 U.S.C. 102(b) as being anticipated by Kosiur.

This rejection for claims 1, 10, 12-15, 17, 26, 28-31, and 33 is adopted for the reasons set forth in the December 8, 2009 request for reexamination which is incorporated by reference (*see Request for Reexamination, pages 25-30 and Appendix C*).

The rejection of claims 4, 20, and 35 as anticipated by Kosiur, as proposed in the request, is not adopted for the following reasons.

Claims 4, 20, and 35 further limit their parent claims by requiring that the response message contain provisioning information for the virtual private network. The response message is defined in claim 1 as "containing the secure computer network address corresponding to the secure domain name" that is received in response to a "query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name." In other words, a query message requests a secure computer network address corresponding to a secure domain name and a response message is received that includes both (1) the secure

computer network address and (2) provisioning information for the virtual private network.

Kosiur fails to teach a response message containing provisioning information for the virtual private network in addition to the secure computer network address as described above and thus fails to anticipate claims 4, 20, and 35. Kosiur teaches the use of DNS in order to resolve domain names into Internet addresses (*Kosiur, Page 296 – map names to addresses*). In doing so, inherently teaches that response messages are received by a client that includes the Internet address associated with a domain name (*Kosiur, Pages 293-296*). However, Kosiur fails to specifically disclose that the response message also includes provisioning information for the VPN. Kosiur never ties together the request for domain name resolution to the provisioning of the VPN. Instead, Kosiur discloses that the DNS system is split into two servers where the addresses of secure internal servers are kept separate on an isolated internal DNS server (*Kosiur, Page 296, internal DNS server).* In teaching this DNS system, Kosiur never specifically discloses that a DNS response message includes both DNS address resolution information and VPN provisioning information.

Issue 4

Requester proposed rejections of Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 as anticipated by Kaufman under 35 U.S.C. §102(a). These proposed rejections are adopted in part.

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 are rejected under 35 U.S.C. 102(a) as being anticipated by Kaufman.

This rejection for claims 1, 10, 12-15, 17, 26, 28-31, and 33, is adopted for the reasons set forth in the December 8, 2009 request for reexamination which is incorporated by reference (*see Request for Reexamination, pages 30-35 and Appendix D).*

The rejection of claims 4, 20, and 35 as anticipated by Kaufman, as proposed in the request, is not adopted for the following reasons.

Claims 4, 20, and 35 further limit their parent claims by requiring that the response message contain provisioning information for the virtual private network. The response message is defined in claim 1 as "containing the secure computer network address corresponding to the secure domain name" that is received in response to a "query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name." In other words, a query message requests a secure computer network address corresponding to a secure domain name and a response message is received that includes both (1) the secure computer network address and (2) provisioning information for the virtual private network.

Kaufman fails to teach a response message containing provisioning information for the virtual private network in addition to the secure computer network address as described above and thus fails to anticipate claims 4, 20, and 35. Kaufman teaches the

use of DNS in order to resolve the addresses of secure domain names and a response message that includes a secure computer network address (*see Kaufman, Page 127 - translate between human comprehensible addresses and IP network addresses)*. Kaufman further teaches the use of messages in order to provision a network connection to carry specified traffic from a sender to a destination (*Kaufman, Page 121 - RSVP signaling protocol)*. However, Kaufman fails to teach the provisioning resulting in a response message sent back to the client that carries provisioning information. Further, Kaufman fails to tie the provisioning to DNS by failing to teach that the response message contains both DNS address resolution information and VPN information.

Issue 5

Requester proposed rejections of Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 as obvious over Kaufman in view of Galvin under 35 U.S.C. §103(a). These proposed rejections are adopted in part.

Claims 1, 10, 12-15, 17, 26, 28-31, and 33, are rejected under 35 U.S.C. 103(a) as being obvious over Kaufman in view of Galvin.

This rejection for claims 1, 10, 12-15, 17, 26, 28-31, and 33, is adopted for the reasons set forth in the December 8, 2009 request for reexamination which is incorporated by reference (*see Request for Reexamination, pages 36-41 and Appendix E)*.

The rejection of claims 4, 20, and 35 as obvious over Kaufman in view of Galvin, as proposed in the request, is not adopted for the following reasons.

Claims 4, 20, and 35 further limit their parent claims by requiring that the response message contain provisioning information for the virtual private network. The response message is defined in claim 1 as "containing the secure computer network address corresponding to the secure domain name" that is received in response to a "query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name." In other words, a query message requests a secure computer network address corresponding to a secure domain name and a response message is received that includes both (1) the secure computer network address and (2) provisioning information for the virtual private network.

Kaufman and Galvin fail to teach a response message containing provisioning information for the virtual private network in addition to the secure computer network address as described above and thus fails to render claims 4, 20, and 35 obvious. Kaufman teaches the use of DNS in order to resolve the addresses of secure domain names and a response message that includes a secure computer network address (*see Kaufman, Page 127 - translate between human comprehensible addresses and IP network addresses)*. Kaufman further teaches the use of messages in order to provision a network connection to carry specified traffic from a sender to a destination (*Kaufman, Page 121 - RSVP signaling protocol)*. However, Kaufman fails to teach the

provisioning resulting in a response message sent back to the client that carries provisioning information. Further, Kaufman fails to tie the provisioning to DNS by failing to teach that the response message contains both DNS address resolution information and VPN information.

On the other hand, Galvin is directed to a secure DNS system that enhances the security of the DNS system by digitally securing DNS records. Galvin also fails to teach a response message containing provisioning information for the virtual private network in addition to the secure computer network. Instead, Galvin teaches a DNS response message that includes a secure computer network address, but does not include any VPN response messages (*Galvin, §3.2, resolve to user message includes IP address).*

Issue 6

Requester proposed rejections of Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 as anticipated by Gauntlet under 35 U.S.C. §102(a). These proposed rejections are adopted in part.

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 are rejected under 35 U.S.C. 102(a) as being anticipated by Gauntlet.

This rejection for claims 1, 10, 12-15, 17, 26, 28-31, and 33 is adopted for the reasons set forth in the December 8, 2009 request for reexamination which is incorporated by reference (*see Request for Reexamination, pages 40-45 and Appendix F).*

The rejection of claims 4, 20, and 35 as anticipated by Gauntlet, as proposed in the request, is not adopted for the following reasons.

Claims 4, 20, and 35 further limit their parent claims by requiring that the response message contain provisioning information for the virtual private network. The response message is defined in claim 1 as "containing the secure computer network address corresponding to the secure domain name" that is received in response to a "query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name." In other words, a query message requests a secure computer network address corresponding to a secure domain name and a response message is received that includes both (1) the secure computer network address and (2) provisioning information for the virtual private network.

Gauntlet fails to teach a response message containing provisioning information for the virtual private network in addition to the secure computer network address as described above and thus fails to anticipate claims 4, 20, and 35. Gauntlet inherently discloses a response message that returns a resolved computer network address by teaching the use of the DNS system to resolve computer addresses (*Gauntlet - Pages 1-8*). However, Gauntlet fails to teach the response message including any information relating to VPN provisioning. Thus, Gauntlet fails to anticipate claims 4, 20, and 35.

Issue 7

Requester proposed rejections of Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 as rendered obvious by the combination of Hands-On in view of Installing NT under 35 U.S.C. 103(a). These proposed rejections are adopted in part.

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hands-On in view of Installing NT.

This rejection for claims 1, 10, 12-15, 17, 26, 28-31, and 33 is adopted for the reasons set forth in the December 8, 2009 request for reexamination which is incorporated by reference (*see Request for Reexamination, pages 45-52 and Appendix G*).

The rejection of claims 4, 20, and 35 as unpatentable over Hands-On in view of Installing NT, as proposed in the request, is not adopted for the following reasons.

Claims 4, 20, and 35.

Claims 4, 20, and 35 further limit their parent claims by requiring that the response message contain provisioning information for the virtual private network. The response message is defined in claim 1 as "containing the secure computer network address corresponding to the secure domain name" that is received in response to a "query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name." In other words, a query message requests a secure computer network address corresponding to a secure

domain name and a response message is received that includes both (1) the secure computer network address and (2) provisioning information for the virtual private network.

Both Hands-On and Installing NT fail to teach a response message containing provisioning information for the virtual private network in addition to the secure computer network address as described above. Instead, Hands-On teaches a DNUS name server that performs name resolution when it receives a DNS resolution query from a client (*Hands-On, Page 401)*. In response to the DNS resolution query, the domain name is resolved to an address and is returns (*Hands-On, Page 401)*. However, Hands-On does not specifically disclose that VPN provisioning information is included in that DNS response. Installing NT does not remedy Hands-On lack of teaching regarding the VPN provisioning information. Installing NT teaches the method of setting up a VPN by using Windows NT phonebook feature where the user enters the necessary VPN information including addresses, domain names, and network protocols (*Installing NT, Pages 20-23)*. Installing NT does not teach the return of provisioning information to the client nor does Installing NT teach the return of provisioning information along with a DNS address resolution information in a response message.

Issue 8

Requester proposed rejections of Claims 1, 10, 12-15, 17, 26, 28-31, and 33 as anticipated by Microsoft VPN under 35 U.S.C. §102(a). These proposed rejections are adopted in part.

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 are rejected under 35 U.S.C. 102(a) as being anticipated by Microsoft VPN.

This rejection for claims 1, 10, 12-15, 17, 26, 28-31, and 33, is adopted for the reasons set forth in the December 8, 2009 request for reexamination which is incorporated by reference (*see Request for Reexamination, pages 52-56 and Appendix H).*

CORRESPONDENCE

All correspondence relating to this inter partes reexamination proceeding should be directed:

By EFS: Registered users may submit via the electronic filing system EFS-Web, at https://sportal.uspto.gov/authenticate/authenticateuserlocalepf.html.

By Mail to:
Mail Stop *Inter Partes* Reexam
Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to:
(571) 273-9900
Central Reexamination Unit

By hand:
Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

For EFS-Web transmissions, 37 CFR 1.8(a)(1)(i) (C) and (ii) states that correspondence (except for a request for reexamination and a corrected or replacement request for reexamination) will be considered timely filed if (a) it is transmitted via the Office's electronic filing system in accordance with 37 CFR 1.6(a)(4), and (b) includes a certificate of transmission for each piece of correspondence stating the date of transmission, which is prior to the expiration of the set period of time in the Office action.

Any inquiry concerning this communication or earlier communications from the Examiner, or as to the status of this proceeding, should be directed to the Central Reexamination Unit at telephone number (571) 272-7705.

Signed:

/Andrew Nalven/

Andrew Nalven
CRU Examiner
GAU 3992
(571) 272-3839

Conferee: ESK

Conferee: AJK

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-09)
Approved for use through 02/28/2009. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	2009-11-25
	First Named Inventor	LARSON, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	3755-121

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Patent citation information please click the Add button.						

U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Published Application citation information please click the Add button.						

FOREIGN PATENT DOCUMENTS								
Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐
If you wish to add additional Foreign Patent Document citation information please click the Add button								

NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

EFS Web 2.1.10

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	2009-11-25
	First Named Inventor	LARSON, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	3755-121

AM	1	Exhibit 2 "Aventail Connect v3.1/v2.6 Administrator's Guide", pgs. 1-120, 1998-1999.	☐
	2	Exhibit 3, "Windows NT Server, Virtual Private Network: An Overview", pgs. 1-28, 1998.	☐
	3	Exhibit 4, "Network Working Group Request For Comments 1035", pgs. 1-56, 1987.	☐
	4	Exhibit 5, "Kuslur" Building and Managing Virtual Private Networks, pgs 1-396, 1998.	☐
	5	Exhibit 6, "Kaufman et al.," Implementing IPsec, pgs. 1-280, 1999.	☐
	6	Exhibit 7, "James Galvin" Public Key Distribution Secure DNS, pgs. 1-12, 1998.	☐
	7	Exhibit 8A, "Gauntlet Firewall for Windows NT Administrator's Guide, pgs 1-137, 1998-1999.	☐
	8	Exhibit 8B, "Gauntlet Firewall for Windows NT Administrator's Guide, pgs. 138-275, 1998-1999.	☐
	9	Exhibit 9, "Windows NT Technical Support: Hands On, Self Paced Training for Supporting Version 4.0", pgs. 1-106, 1998.	☐
	10	Exhibit 10, "Microsoft Windows NT Server, Whitepaper: Installing, Configuring, and Using PPTP with Mircosoft Clients and Servers, pgs. 1-30, 1997.	☐
	11	Exhibit 11, "Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources, pgs. 1-218, 2000.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	2009-11-25
	First Named Inventor	LARSON, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	3755-121

If you wish to add additional non-patent literature document citation information please click the Add button			
EXAMINER SIGNATURE			
Examiner Signature		Date Considered	12/17/09

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language translation is attached.

Reexamination	Application/Control No.	Applicant(s)/Patent Under Reexamination
	95/001,270	7188180
	Certificate Date	Certificate Number

Requester Correspondence Address: ☐ Patent Owner ☒ Third Party
Rothwell, Figg, Ernst & Manbeck, P.C. 1425 K Street NW Suite 800 Washington, DC 20005

LITIGATION REVIEW ☒	aln (examiner initials)	1/7/2010 (date)
Case Name		Director Initials
VirnetX et al v. Microsoft - 6:07-cv-00080-LED		Lee Rear FS CM

COPENDING OFFICE PROCEEDINGS	
TYPE OF PROCEEDING	NUMBER
1.	
2.	
3.	
4.	

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	95001270	7188180
	Examiner	Art Unit
		3999

SEARCHED			
Class	Subclass	Date	Examiner
709	227		

SEARCH NOTES		
Search Notes	Date	Examiner
Reviewed patented file's prosecution history	1/6/10	aln

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

REEXAM CONTROL NUMBER	FILING OR 371 (c) DATE	PATENT NUMBER
95/001,270	12/08/2009	7188180

CONFIRMATION NO. 2128

ASSIGNMENT NOTICE

22907
BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

Date Mailed: 12/10/2009

NOTICE OF ASSIGNMENT OF *INTER PARTES* REEXAMINATION REQUEST

The above-identified request for *inter partes* reexamination has been assigned to Art Unit 3992. All future correspondence in this proceeding should be identified by the control number listed above and directed to: Mail Stop Inter Partes Reexam, Commissioner for Patents, P.O. Box 1450, Alexandria VA 22313-1450.

A copy of this Notice is being sent to the latest attorney or agent of record in the patent file or, if none is of record, to all owners of record. (See 37 CFR 1.33(c).) If the addressee is not, or does not represent, the current owner, he or she is required to forward all communications regarding this proceeding to the current owner(s)

(MPEP 2222). An attorney or agent receiving this communication who does not represent the current owner(s) may wish to seek to withdraw pursuant to 37 CFR 1.36 in order to avoid receiving future communications. If the address of the current owner(s) is unknown, this communication should be returned with the request to withdraw pursuant to Section 1.36.

cc: Third Party Requester
ROTHWELL, FIGG, ERNST & MANBECK, P.C.
1425 K STREET N.W.
SUITE 800
WASHINGTON, DC 20005

/sdstevenson/

Legal Instruments Examiner
Central Reexamination Unit 571-272-7705; FAX No. 571-273-9900

Petitioner Apple Inc. - Exhibit 1002, p. 401

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

REEXAM CONTROL NUMBER	FILING OR 371 (c) DATE	PATENT NUMBER
95/001,270	12/08/2009	7188180

CONFIRMATION NO. 2128

REEXAM ASSIGNMENT NOTICE

ROTHWELL, FIGG, ERNST & MANBECK, P.C.
1425 K STREET N.W.
SUITE 800
WASHINGTON, DC 20005

Date Mailed: 12/10/2009

NOTICE OF *INTER PARTES* REEXAMINATION REQUEST FILING DATE

Requester is hereby notified that the filing date of the request for *inter partes* reexamination is 12/08/2009, the date that the filing requirements of 37 CFR § 1.915 were received.

A decision on the request for *inter partes* reexamination will be mailed within three months from the filing date of the request for *inter partes* reexamination. (See 37 CFR 1.923.)

A copy of this Notice is being sent to the person identified by the requestor as the patent owner. Further patent owner correspondence will be with the latest attorney or agent of record in the patent file. (See 37 CFR 1.33.) Any paper filed should include a reference to the present request for *inter partes* reexamination (by Reexamination Control Number) and should be addressed to: Mail Stop Inter Partes Reexam, Commissioner for Patents, P.O. Box 1450, Alexandria VA 22313-1450.

cc: Patent Owner
22907
BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

/sdstevenson/

Legal Instruments Examiner
Central Reexamination Unit 571-272-7705; FAX No. 571-273-9900

Petitioner Apple Inc. - Exhibit 1002, p. 402

Patent Assignment Abstract of Title

Total Assignments: 2

Application #: 10702486 **Filing Dt:** 11/07/2003 **Patent #:** 7188180 **Issue Dt:** 03/06/2007
PCT #: NONE **Publication #:** US20040107285 **Pub Dt:** 06/03/2004
Inventors: Victor Larson, Robert Dunham Short III, Edmund Colby Munger, Michael Williamson
Title: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

Assignment: 1

Reel/Frame: 014679 / 0947 **Received:** 11/14/2003 **Recorded:** 11/07/2003 **Mailed:** 06/03/2004 **Pages:** 3
Conveyance: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).
Assignors: LARSON, VICTOR **Exec Dt:** 11/06/2003
SHORT, ROBERT DUNHAM III **Exec Dt:** 10/27/2003
MUNGER, EDMUND COLBY **Exec Dt:** 11/05/2003
WILLIAMSON, MICHAEL **Exec Dt:** 11/05/2003
Assignee: SCIENCE APPLICATIONS INTERNATIONAL CORPORATION
10260 CAMPUS POINT DRIVE
SAN DIEGO, CALIFORNIA 92121
Correspondent: BANNER & WITCOFF, LTD.
ROSS A. DANNENBERG
1001 G STREET, N.W., 11TH FLOOR
WASHINGTON, DC 20001

Assignment: 2

Reel/Frame: 018757 / 0326 **Received:** 01/10/2007 **Recorded:** 01/10/2007 **Mailed:** 01/16/2007 **Pages:** 5
Conveyance: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).
Assignor: SCIENCE APPLICATIONS INTERNATIONAL CORPORATION **Exec Dt:** 12/21/2006
Assignee: VIRNETX INC.
5615 SCOTTS VALLEY DRIVE, SUITE 110
SCOTTS VALLEY DRIVE, CALIFORNIA 95066
Correspondent: BANNER & WITCOFF, LTD.
1001 G STREET, N.W. - 11TH FLOOR
WASHINGTON, D.C. 20001-4597

Search Results as of: 12/09/2009 04:19 PM

If you have any comments or questions concerning the data displayed, contact PRD / Assignments at 571-272-3350.
Web interface last modified: October 18, 2008 v.2.0.1

Litigation Search Report CRU 3999

Reexam Control No. 95/001,270

TO: MARK REINHART **Location: CRU** **Art Unit: 3992** **Date: 12/09/09**	**From: MANUEL SALDANA** **Location: CRU 3999** **MDW 7C55** **Phone: (571) 272-7740** **MANUEL.SALDANA@uspto.gov**

Search Notes

Litigation was NOT found for US Patent Number: **7,188,180.**

1) I performed a KeyCite Search in Westlaw, which retrieves all history on the patent including any litigation.

2) I performed a search on the patent in Lexis CourtLink for any open dockets or closed cases.

3) I performed a search in Lexis in the Federal Courts and Administrative Materials databases for any cases found.

4) I performed a search in Lexis in the IP Journal and Periodicals database for any articles on the patent.

5) I performed a search in Lexis in the news databases for any articles about the patent or any articles about litigation on this patent.

Date of Printing: Dec 09, 2009

KEYCITE

C US PAT 7188180 METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK, Assignee: VimetX, Inc. (Mar 06, 2007)

History

Direct History

=> 1 METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK, US PAT 7188180, 2007 WL 665444 (U.S. PTO Utility Mar 06, 2007) (NO. 10/702486)

Patent Family

2 INFORMATION TRANSMISSION INVOLVES COMPARING DISCRIMINATOR VALUE FOR EACH RECEIVED DATA PACKET WITH SET OF VALID DISCRIMINATOR VALUES, ACCEPTING RECEIVED DATA PACKET FOR FURTHER PROCESSING WHILE DETECTING MATCH, Derwent World Patents Legal 2000-399393

Assignments

3 Action: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS). Number of Pages: 005, (DATE RECORDED: Jan 10, 2007)

4 Action: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS). Number of Pages: 003, (DATE RECORDED: Nov 07, 2003)

Patent Status Files

.. Certificate of Correction, (OG DATE: Aug 28, 2007)

Prior Art (Coverage Begins 1976)

C 6 AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY, US PAT 7010604Assignee: Science Applications International, (U.S. PTO Utility 2006)

C 7 AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY, US PAT 6502135Assignee: Science Applications International, (U.S. PTO Utility 2002)

C 8 APPARATUS AND METHOD FOR ESTABLISHING A CRYPTOGRAPHIC LINK BETWEEN ELEMENTS OF A SYSTEM; US PAT 5787172Assignee: The Merdan Group, Inc., (U.S. PTO Utility 1998)

C 9 AUTOCONFIGURABLE METHOD AND SYSTEM HAVING AUTOMATED DOWNLOADING, US PAT 5870610Assignee: Siemens Business Communication Systems,, (U.S. PTO Utility

© 2009 Thomson Reuters. All rights reserved.

1999)

C 10 CRYPTOGRAPHIC KEY MANAGEMENT APPARATUS AND METHOD, US PAT 5341426Assignee: Motorola, Inc., (U.S. PTO Utility 1994)

C 11 DOMAIN NAME ROUTING, US PAT 6119171Assignee: IP Dynamics, Inc., (U.S. PTO Utility 2000)

C 12 DOMAIN NAME SYSTEM LOOKUP ALLOWING INTELLIGENT CORRECTION OF SEARCHES AND PRESENTATION OF AUXILIARY INFORMATION, US PAT 6332158 (U.S. PTO Utility 2001)

C 13 DYNAMIC NETWORK ADDRESS UPDATING, US PAT 6243749Assignee: Cisco Technology, Inc., (U.S. PTO Utility 2001)

C 14 FIREWALL PROVIDING ENHANCED NETWORK SECURITY AND USER TRANSPARENCY, US PAT 6052788Assignee: Network Engineering Software, Inc., (U.S. PTO Utility 2000)

C 15 FIREWALL PROVIDING ENHANCED NETWORK SECURITY AND USER TRANSPARENCY, US PAT 5898830Assignee: Network Engineering Software, (U.S. PTO Utility 1999)

C 16 MANAGED NETWORK DEVICE SECURITY METHOD AND APPARATUS, US PAT 5905859Assignee: International Business Machines, (U.S. PTO Utility 1999)

C 17 METHOD AND APPARATUS FOR AUTOMATED NETWORK-WIDE SURVEILLANCE AND SECURITY BREACH INTERVENTION, US PAT 5796942Assignee: Computer Associates International, Inc., (U.S. PTO Utility 1998)

C 18 METHOD AND APPARATUS FOR CLIENT-HOST COMMUNICATION OVER A COMPUTER NETWORK, US PAT 6119234Assignee: Sun Microsystems, Inc., (U.S. PTO Utility 2000)

C 19 METHOD AND APPARATUS FOR CONFIGURING A VIRTUAL PRIVATE NETWORK, US PAT 6226751Assignee: VPNet Technologies, Inc., (U.S. PTO Utility 2001)

C 20 METHOD AND APPARATUS FOR DETECTING AND IDENTIFYING SECURITY VULNERABILITIES IN AN OPEN NETWORK COMPUTER COMMUNICATION SYSTEM, US PAT 5892903Assignee: Internet Security Systems, Inc., (U.S. PTO Utility 1999)

C 21 METHOD AND APPARATUS FOR AN INTERNET PROTOCOL (IP) NETWORK CLUSTERING SYSTEM, US PAT 6006259Assignee: Network Alchemy, Inc., (U.S. PTO Utility 1999)

C 22 METHOD AND APPARATUS FOR A KEY-MANAGEMENT SCHEME FOR INTERNET PROTOCOLS, US PAT 5588060Assignee: Sun Microsystems, Inc., (U.S. PTO Utility 1996)

C 23 METHOD AND APPARATUS FOR MANAGING A VIRTUAL PRIVATE NETWORK, US PAT 6079020Assignee: VPNet Technologies, Inc., (U.S. PTO Utility 2000)

C 24 METHOD AND APPARATUS FOR PROVIDING NETWORK ACCESS CONTROL USING A DOMAIN NAME SYSTEM, US PAT 6256671Assignee: Nortel Networks Limited, (U.S. PTO Utility 2001)

C 25 METHOD AND APPARATUS FOR PROVIDING A VIRTUAL PRIVATE NETWORK, US PAT 6092200Assignee: Novell, Inc., (U.S. PTO Utility 2000)

C 26 METHOD AND PROTOCOL FOR DISTRIBUTED NETWORK ADDRESS TRANSLATION, US PAT 6353614Assignee: 3Com Corporation, (U.S. PTO Utility 2002)

© 2009 Thomson Reuters. All rights reserved.

C 27 METHOD AND SYSTEM FOR AUTOMATIC DISCOVERY OF NETWORK SERVICES, US PAT 6286047Assignee: Hewlett-Packard Company, (U.S. PTO Utility 2001)

C 28 MULTI-ACCESS VIRTUAL PRIVATE NETWORK, US PAT 6158011Assignee: V-One Corporation, (U.S. PTO Utility 2000)

C 29 NETWORK COMMUNICATIONS ADAPTER WITH DUAL INTERLEAVED MEMORY BANKS SERVICING MULTIPLE PROCESSORS, US PAT 4933846Assignee: Network Systems Corporation, (U.S. PTO Utility 1990)

C 30 NETWORK WITH SECURE COMMUNICATIONS SESSIONS, US PAT 5689566 (U.S. PTO Utility 1997)

H 31 POLICY CACHING METHOD AND APPARATUS FOR USE IN A COMMUNICATION DEVICE BASED ON CONTENTS OF ONE DATA UNIT IN A SUBSET OF RELATED DATA UNITS, US PAT 5842040Assignee: Storage Technology Corporation, (U.S. PTO Utility 1998)

C 32 SECURE DELIVERY OF INFORMATION IN A NETWORK, US PAT 6178505Assignee: Internet Dynamics, Inc., (U.S. PTO Utility 2001)

C 33 SYSTEM AND METHOD FOR DETECTING AND PREVENTING SECURITY, US PAT 5805801Assignee: International Business Machines, (U.S. PTO Utility 1998)

C 34 SYSTEM AND METHOD FOR MANAGING SECURITY OBJECTS, US PAT 6330562Assignee: International Business Machines, (U.S. PTO Utility 2001)

C 35 SYSTEM FOR PACKET FILTERING OF DATA PACKETS AT A COMPUTER NETWORK INTERFACE, US PAT 5878231Assignee: Sun Microsystems, Inc., (U.S. PTO Utility 1999)

C 36 SYSTEM, METHOD AND ARTICLE OF MANUFACTURE FOR MULTIPLE-ENTRY POINT VIRTUAL POINT OF SALE ARCHITECTURE, US PAT 6178409Assignee: VeriFone, Inc., (U.S. PTO Utility 2001)

C 37 VIRTUAL PRIVATE NETWORK SYSTEM OVER PUBLIC MOBILE DATA NETWORK AND VIRTUAL LAN, US PAT 6016318Assignee: NEC Corporation, (U.S. PTO Utility 2000)

© 2009 Thomson Reuters. All rights reserved.

Exhibit B3, Part 4

File History of Reexamination Control No. 95/001,270, reexamination of U.S. 7,188,180 requested by Microsoft Corp.

Customer No.: 000027683

Haynes and Boone, LLP
IP Section
2323 Victory Avenue, Suite 700
Dallas, Texas 75219
Telephone [214] 651.5000
Fax [214] 200.0853

Patent Search 7188180 12/9/2009

No cases found.

Return to Search

(Charges for search still apply)

LexisNexis® | About LexisNexis | Terms & Conditions | Pricing | Privacy | Customer Support - 1-888-311-1966
Copyright © 2009 LexisNexis®. All rights reserved.

Search

Select Search Type and Enter Search Terms

Terms & Connectors | Natural Language | Easy Search™ | Semantic Search What's this?

PATNO= 7188180

Suggest terms for my search | Search

Check spelling

Restrict by Document Segment

Select a document segment, enter search terms for the segment, then click Add.

Select a Segment | Add

Note: Segment availability differs between sources. Segments may not be applied consistently across sources.

Restrict by Date

No Date Restrictions | From | To | Date formats...

Search Connectors

and	and	w/p	in same paragraph
or	or	w/seg	in same segment
w/N	within N words	w/s	in same sentence
pre/N	precedes by N words	and not	and not

> More Connectors & Commands...

How Do I...?

> Combine sources?
> Restrict by date?
> Restrict by document segment?
> Use wildcards as placeholders for one or more characters in a search term?

View Tutorials

LexisNexis® About LexisNexis | Terms & Conditions | Contact Us

Copyright © 2009 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

702486 (10) 7188180 March 6, 2007 ,

UNITED STATES PATENT AND TRADEMARK OFFICE GRANTED PATENT

7188180

Get Drawing Sheet 1 of 40

Access PDF of Official Patent *

Order Patent File History / Wrapper from REEDFAX®

Link to Claims Section

June 3, 2004 ,

Method for establishing secure communication link between computers of virtual private network

INVENTOR: Larson, Victor - Fairfax, VIRGINIA , , United States of America (US) ; Short, III, Robert Durham - Leesburg, VIRGINIA , , United States of America (US) ; Munger, Edmund Colby - Crownsville, MARYLAND , , United States of America (US) ; Williamson, Michael - South Riding, VIRGINIA , , United States of America (US)

APPL-NO: 702486 (10)

FILED-DATE: November 7, 2003

GRANTED-DATE: March 6, 2007 ,

CORE TERMS: packet, computer, server, network, message, router, sync, node, transmitter, receiver ...

ENGLISH-ABST:

A technique is disclosed for establishing a secure communication link between a first computer and a second computer over a computer network. Initially, a secure communication mode of communication is enabled at a first computer without a user entering any cryptographic information for establishing the secure communication mode of communication. Then, a secure communication link is established between the first computer and a second computer over a computer network based on the enabled secure communication mode of communication. The secure communication link is a virtual private network communication link over the computer network in which one or more data values that vary according to a pseudo-random sequence are inserted into each data packet.

Petitioner Apple Inc. - Exhibit 1002, p. 411

LexisNexis® About LexisNexis | Terms & Conditions | Contact Us
Copyright © 2009 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

Search

Select Search Type and Enter Search Terms

Terms & Connectors | Natural Language | Easy Search™

7188180 OR 7,188,180

Suggest terms for my search

Search

Check spelling

Restrict by Document Segment

Select a document segment, enter search terms for the segment, then click Add.

Select a Segment | Add

Note: Segment availability differs between sources. Segments may not be applied consistently across sources.

Restrict by Date

No Date Restrictions | From | To | Date formats...

Search Connectors

and	and	w/p	in same paragraph
or	or	w/seg	in same segment
w/N	within N words	w/s	in same sentence
pre/N	precedes by N words	and not	and not

> More Connectors & Commands...

How Do I...?

> Combine sources?
> Restrict by date?
> Restrict by document segment?
> Use wildcards as placeholders for one or more characters in a search term?

View Tutorials

LexisNexis® About LexisNexis | Terms & Conditions | Contact Us

Copyright © 2009 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

Source: Legal > / . . . / > Patent Cases from Federal Courts and Administrative Materials
Terms: 7188180 OR 7,188,180 (Edit Search | Suggest Terms for My Search)

Select for FOCUS™ or Delivery

1. VirnetX, Inc. v. Microsoft Corp., CASE NO. 6:07 CV 80, UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TEXAS, TYLER DIVISION, 2009 U.S. Dist. LEXIS 65667, July 30, 2009, Decided, July 30, 2009, Filed

   CORE TERMS: network, domain, web, virtual, site, specification, server, user, target, proxy ...

2. VirnetX, Inc. v. Microsoft Corp., CASE NO. 6:07 CV 80, UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TEXAS, TYLER DIVISION, 2008 U.S. Dist. LEXIS 94854, June 3, 2008, Decided, June 4, 2008, Filed, Patent Interpreted by VirnetX, Inc. v. Microsoft Corp., 2009 U.S. Dist. LEXIS 65667 (E.D. Tex., July 30, 2009)

   CORE TERMS: patent-in-suit, patent, license, infringement, grantor, patent rights, substantial rights, grantee, joinder, join ...

Source: Legal > / . . . / > Patent Cases from Federal Courts and Administrative Materials
Terms: 7188180 OR 7,188,180 (Edit Search | Suggest Terms for My Search)
View: Cite
Date/Time: Wednesday, December 9, 2009 - 4:38 PM EST

* Signal Legend:
- Warning: Negative treatment is indicated
- Questioned: Validity questioned by citing refs
- Caution: Possible negative treatment
- Positive treatment is indicated
- Citing Refs. With Analysis Available
- Citation information available

* Click on any *Shepard's* signal to *Shepardize®* that case.

Copyright © 2009 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

Search

Select Search Type and Enter Search Terms

Terms & Connectors | Natural Language | Easy Search™

7188180 OR 7,188,180

Suggest terms for my search | Search

Check spelling

Restrict by Document Segment

Select a document segment, enter search terms for the segment, then click Add.

Select a Segment | Add

Note: Segment availability differs between sources. Segments may not be applied consistently across sources.

Restrict by Date

No Date Restrictions | From | To | Date formats...

Search Connectors

and	and	w/p	in same paragraph
or	or	w/seg	in same segment
w/N	within N words	w/s	in same sentence
pre/N	precedes by N words	and not	and not

> More Connectors & Commands...

How Do I...?

> Combine sources?
> Restrict by date?
> Restrict by document segment?
> Use wildcards as placeholders for one or more characters in a search term?

View Tutorials

LexisNexis® About LexisNexis | Terms & Conditions | Contact Us

Copyright © 2009 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

No Documents Found

No documents were found for your search terms

"7188180 OR 7,188,180"

Click "Save this search as an Alert" to schedule your search to run in the future.

- OR -

Click "Edit Search" to return to the search form and modify your search.

Suggestions:

- Check for spelling errors .
- Remove some search terms.
- Use more common search terms, such as those listed in "Suggested Words and Concepts"
- Use a less restrictive date range.

Save this Search as an Alert | Edit Search

LexisNexis® About LexisNexis | Terms & Conditions | Contact Us
Copyright © 2009 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

Search

Select Search Type and Enter Search Terms

Terms & Connectors | Natural Language | Easy Search™

7188180 OR 7,188,180

Suggest terms for my search | Search

Check spelling

Restrict by Document Segment

Select a document segment, enter search terms for the segment, then click Add.

Select a Segment | Add

Note: Segment availability differs between sources. Segments may not be applied consistently across sources.

Restrict by Date

No Date Restrictions | From | To | Date formats...

Search Connectors

and	and	w/p	in same paragraph
or	or	w/seg	in same segment
w/N	within N words	w/s	in same sentence
pre/N	precedes by N words	and not	and not

> More Connectors & Commands...

How Do I...?

> Combine sources?
> Restrict by date?
> Restrict by document segment?
> Use wildcards as placeholders for one or more characters in a search term?

View Tutorials

Copyright © 2009 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

1. Virginia, Maryland Inventors Develop Secure Computer Network Address Access Method, US Fed News, March 19, 2007 Monday 11:41 PM EST, , 293 words, US Fed News, Alexandria, Va.

2. Third Quarter Free Cash Flow Turns Negative for AMCON, Cashflow news, November 30, 2006 Thursday 6:02 PM EST, , 286 words

Source: Legal > / . . . / > News, All (English, Full Text)
Terms: 7188180 OR 7,188,180 (Edit Search | Suggest Terms for My Search)
View: Cite
Date/Time: Wednesday, December 9, 2009 - 4:38 PM EST

Copyright © 2009 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

Patent
Attorney Docket No.: 3755-121

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent No: 7,188,180	)	
	)	
Victor LARSON, et al.	)	Reexam Control
	)	No. 95/001,270
Issued: March 6, 2007	)	
	)	
Filed: November 7, 2003	)	
	)	
Title: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK	)	

REPLACEMENT REQUEST FOR *INTER PARTES* REEXAMINATION OF PATENT

Attn: Mail Stop *Inter Partes* Reexam
Central Reexamination Unit (CRU)
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Replacement Request for *Inter Partes* Reexamination is being filed in response the Notice of Failure to Comply with *Inter Partes* Reexamination Request Filing Requirements, dated December 3, 2009, objecting to the prior Request for *Inter Partes* Reexamination of claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of U.S. Patent No. 7,188,180. The present reexamination request corrects the deficiencies of the November 25, 2009 request by expressly pointing out each substantial new question of patentability and providing a detailed explanation of the pertinency and manner of applying the printed publications to every claim for which reexamination is requested.

Reexamination is requested of claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of U.S. Patent No. 7,188,180 ("the '180 patent") to Larson et al., pursuant to 35 U.S.C. §§ 311 - 316 and 37 C.F.R. § 1.902 *et seq*. The '180 patent is entitled "Method for Establishing Secure

Communication Link Between Computers of Virtual Private Network" and issued March 6, 2007, from U.S. Patent Application No. 10/702,486, filed November 7, 2003. The requestor is Microsoft Corporation, and the '180 patent has not been previously reexamined.

Request for *Inter Partes* Reexamination

Requestor respectfully submits that there are substantial new questions regarding the patentability of claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of the '180 patent. These substantial new questions of patentability are based on previously uncited, and thus unconsidered, prior art references that render each of these claims unpatentable. Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of the '180 patent are unpatentable in view of these new prior art references under 35 U.S.C. § 102 or 35 U.S.C. § 103. Accordingly, Requestor respectfully requests that this Request for Inter Partes Reexamination be granted. This Request for Inter Partes Reexamination satisfies the requirements of 37 C.F.R. § 1.915(b)(1) through (8) as follows:

37 C.F.R. § 1.915(b)(1): Reexamination of claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of U.S. Patent No. 7,188,180 to Larson, et al. is requested.

37 C.F.R. § 1.915(b)(2): This reexamination request is based on the prior art references listed in Section III.

37 C.F.R. § 1.915(b)(3): A statement of each substantial new question of patentability is presented in Section II. A detailed explanation of the pertinency and manner of applying the prior art to each claim element in the requested claims is provided in Section V, based on the claim charts presented as Appendices A - H.

37 C.F.R. § 1.915(b)(4): Copies of the references relied upon in paragraphs (b)(1) through (3) above are submitted herein as Exhibits 2 - 11. The references relied upon are listed in an equivalent of a PTO Form 1449, which is submitted herewith as Exhibit 12.

37 C.F.R. § 1.915(b)(5): A copy of the entire '180 patent is submitted as Exhibit 1.

37 C.F.R. § 1.915(b)(6): Requester certifies this entire replacement reexamination request was served in its entirety on the purported patent owner at:

VirnetX, Inc.
c/o Banner & Witcoff, Ltd.
1100 13th Street, N.W., Suite 1200

Petitioner Apple Inc. - Exhibit 1002, p. 420

Washington, D.C. 20005-4051

and

VirnetX, Inc.
5615 Scotts Valley Drive, Suite 110
Scotts Valley, Ca 95066

on the 8th day of December, 2009.

37 C.F.R. § 1.915(b)(7): Requestor certifies that this is a new reexamination request, and that therefore the estoppel provisions of 37 C.F.R. § 1.907 do not prohibit this Request.
37 C.F.R. § 1.915(b)(8): The real party in interest for this request is Microsoft Corporation.

As noted above, this request for *Inter Partes* Reexamination was initially filed November 25, 2009, and authorization to charge our Deposit Account No. 02-2135 in the amount of $8,800.00 was submitted on that date, pursuant to 37 C.F.R. § 1.20(c)(2), to cover the fee of the Request for *Inter Partes* Reexamination. Accordingly, it is believed that no further fee is due at this time for submitting this replacement request. However, if any fee is required in connection with this resubmission, please charge our Deposit Account No. 02-2135.

Notification of Concurrent Proceedings

Pursuant to 37 C.F.R. § 1.985, Requestor provides notice that the '180 Larson patent is presently involved in a patent infringement action brought in the United States District Court for the Eastern District of Texas, the action having been assigned Case No. 6:07-cv-00080-LED and captioned "VIRNETX, INC. AND SCIENCE APPLICATIONS INTERNATIONAL CORPORATION VS. MICROSOFT CORPORATION." ("the VirnetX case"). Microsoft Corporation is the Requestor of the present Request for Inter Partes Reexamination and, upon information and belief, VirnetX, Inc. is the alleged assignee of the '180 Larson patent.

The Requestor also provides notice that two additional patents in the family of the '180 patent are involved in the above-noticed VirnetX litigation, namely U.S. Patent Nos. 6,502,135 to Munger, et al. and 6,839,759 to Larson, et al. The Requestor is also filing herewith a separate Request for Inter Partes Reexamination of the 6,502,135 Munger et al. patent.

Petitioner Apple Inc. - Exhibit 1002, p. 421

Disclaimer Regarding Claim Construction

In reexamination, the Patent Office must afford the claims the broadest reasonable interpretation consistent with the specification. *In re Yamamoto*, 740 F.2d 1569, 1571 (Fed. Cir. 1984). The legal standards for claim construction in reexamination do not necessarily correspond to the legal standards that are mandated to be used by the courts in litigation. See MPEP §2686.05 (determination of a substantial new question of patentability is made independently of a court's decision on validity because the District Courts and the Patent Office use different standards of proof and claim interpretation); see also *In re Zletz*, 893 F.2d 319, 321, 13 USPQ2d 1320,1321-22 (Fed. Cir. 1989) (during patent examination, the pending claims must be interpreted as broadly as their terms reasonably allow). Requester submits that claim constructions discussed herein for the purposes of demonstrating a substantial new question of patentability are not binding upon Requester in any litigation.

I. Claims for Which Reexamination is Requested

Reexamination is respectfully requested for claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of the '180 patent under 35 U.S.C. §§ 311 - 316 and 37 C.F.R. § 1.902 *et seq*. Claims 1, 17, and 33 are independent claims. Claims 4, 10, and 12-15 depend, directly or ultimately, from independent claim 1; claims 20, 26, and 28-31 depend, directly or ultimately, from independent claim 17; and claim 35 depends directly from independent claim 33.

II. Substantial New Questions of Patentability

The Requestor respectfully submits that there are substantial new questions ("SNQ") regarding the patentability of claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of the '180 patent. Each of these substantial new questions of patentability is based on prior art not cited during prosecution of the '180 patent and which render each of these claims unpatentable. Each of issued claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of the '180 patent are unpatentable in view of these prior art references under 35 U.S.C. § 102 and/or 35 U.S.C. § 103.

On November 21, 2006, a Notice of Allowance and a Notice of Allowability were mailed in the '180 patent application, wherein the Examiner asserted his statement of reasons for allowance:

The prior arts of record do not teach a system and a method for accessing a secure

Petitioner Apple Inc. - Exhibit 1002, p. 422

> computer network address comprising steps of: requesting a secure computer network address from a secure domain name server according to the secure domain name; and using a virtual private network communication link to send an access request message to the secure computer network address.

See Exhibit 14, Notice of Allowance. The statement of reasons for allowance is a paraphrase of independent claim 1 and includes many of the elements of independent claims 17 and 33, of which reexamination is being requested herein. Substantial new questions of patentability are raised because none of the references cited herein were considered by the Examiner during prosecution of the '180 patent application and because these references disclose, separately or in combination, teachings that are different from the prior art of record, and therefore new to the Examiner, that anticipate or render obvious each of the claimed elements that had been asserted by the Examiner to be the reason the claims were allowed. A reasonable Examiner would have found the teachings of these non-cumulative new references important in deciding whether the claims were patentable because the new references disclose the claimed elements that the Examiner believed were missing from the prior art of record, upon which basis the pending '180 patent application claims were allowed. The anticipatory and obviousness teachings of these new prior art references would have been found particularly important to a reasonable Examiner in view of the fact that no art rejection had ever been made during prosecution of the '180 patent application.

III. U.S. Patents and Printed References Which Raise a Substantial New Question of Patentability

Reexamination of claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of the '180 patent is requested in view of the following references:

Exhibit 2. Aventail Administrator's Guide (hereafter "Aventail"), published in 1996 - 1999, before the filing of the '180 patent and qualifies as prior art under 35 U.S.C. § 102(a). Aventail was not considered during prosecution of the '180 patent.

Exhibit 3. Microsoft, Windows NT Server, Virtual Private Networking: An Overview (hereafter "VPN Overview"), published in 1998, before the filing of the '180 patent and qualifies as prior art under 35 U.S.C. § 102(b). VPN Overview was not considered during prosecution of the '180 patent.

Petitioner Apple Inc. - Exhibit 1002, p. 423

Exhibit 4. RFC 1035, published in 1987, before the filing of the '180 patent and qualifies as prior art under 35 U.S.C. § 102(b). RFC 1035 was not considered during prosecution of the '180 patent.

Exhibit 5. David Kosiur, Building and Managing Virtual Private Networks (hereafter "Kosiur"), published in 1998, before the filing of the '180 patent and qualifies as prior art under 35 U.S.C. § 102(b). Kosiur was not considered during prosecution of the '180 patent.

Exhibit 6. Elizabeth Kaufman, Implcmcnting IPscc (hereafter "Kaufman"), published in September 7, 1999, before the filing of the '180 patent and qualifies as prior art under 35 U.S.C. § 102(a). Kaufman was not considered during prosecution of the '180 patent.

Exhibit 7. James Galvin, Public Key Distribution with Secure DNS (hereafter "Galvin"), published in July 1996, before the filing of the '180 patent and qualifies as prior art under 35 U.S.C. § 102(b). Galvin was not considered during prosecution of the '180 patent.

Exhibit 8. Gauntlet Firewall for Windows NT, Administrator's Guide (hereafter "Gauntlet"), published no later than 1999, before the filing of the '180 patent and qualifies as prior art under 35 U.S.C. § 102(a). Gauntlet was not considered during prosecution of the '180 patent.

Exhibit 9. Microsoft Windows NT Technical Support: Hands-On, Self-Paced Training for Support Version 4.0 (hereafter "Hands-On"), published in 1998, before the filing of the '180 patent and qualifies as prior art under 35 U.S.C. § 102(b). Hands-On was not considered during prosecution of the '180 patent.

Exhibit 10. Microsoft Windows NT Server, Whitepaper: Installing, Configuring, and Using PPTP with Microsoft Clients and Servers (hereafter "Installing NT"), published in 1997, before the filing of the '180 patent and qualifies as prior art under 35 U.S.C. § 102(b). Installing NT was not considered during prosecution of the '180 patent.

Exhibit 11. Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources (hereafter "Microsoft VPN"), published in January 1, 2000, before the filing of the

Petitioner Apple Inc. - Exhibit 1002, p. 424

'180 patent and qualifies as prior art under 35 U.S.C. § 102(a). Microsoft VPN was not considered during prosecution of the '180 patent.

These new prior art references are non-cumulative to the prior art considered during the original prosecution of the '180 patent and raise substantial new questions of patentability with respect to at least claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 because they each teach, separately or in combination, the very claimed elements that the Examiner believed were absent in the prior art of record. The detailed explanation of the pertinency and application of the references to the claims is presented in Section V (identified by SNQ and page number in the table below). For each reference, there is an explanation of why it creates a substantial new question of patentability, either alone or in combination with other references, with respect to the claims of the '180 patent. The supporting claim charts illustrating the prior art disclosure from the references can be found in Appendices A-H.

Principal Reference	Substantial New Questions of Patentability Raised Alone Or In Combination With Other References	SNQ #	Page #	Claim Chart
Aventail Administrators Guide	Claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 are unpatentable under 35 U.S.C. § 102(a) for being anticipated by Aventail.	SNQ #1	12	Appendix A
VPN Overview	Claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 are unpatentable under 35 U.S.C. § 103(a) for being obvious over VPN Overview in view of RFC 1035.	SNQ #2	19	Appendix B
Kosiur	Claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 are unpatentable under 35 U.S.C. § 102(b) for being anticipated by Kosiur.	SNQ #3	25	Appendix C
Kaufman	Claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 are unpatentable under 35 U.S.C. § 102(a) for being anticipated by Kaufman.	SNQ #4	30	Appendix D
Kaufman	Claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 are unpatentable under 35 U.S.C. § 103 for being obvious over Kaufman in view of Galvin.	SNQ #5	36	Appendix E
Gauntlet	Claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 are unpatentable under 35 U.S.C. § 102(a) for being anticipated by Gauntlet.	SNQ #6	40	Appendix F
Hands On	Claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 are unpatentable under 35 U.S.C. § 103(a) for being obvious over Hands On in view of Installing NT.	SNQ #7	45	Appendix G

Petitioner Apple Inc. - Exhibit 1002, p. 425

Microsoft VPN	Claims 1, 10, 12 - 15, 17, 26, 28 - 31, and 33 are unpatentable under 35 U.S.C. § 102(a) for being anticipated by Microsoft VPN.	SNQ #8	52	Appendix H

IV. Overview of the '180 Patent, for Which Reexamination is Requested

A. Summary of the Disclosure & the Priority Date of the Claims of the '180 Patent

The '180 patent issued March 6, 2007 from U.S. Patent Application No. 10/702,486 ("the '486 application"), which was filed November 7, 2003. The '486 application is a divisional application of U.S. Patent Application No. 09/558,209, filed April 26, 2000, now abandoned ("the '209 application"). The '209 application is a continuation-in-part ("CIP") application of U.S. Patent Application No. 09/504,783, filed February 15, 2000, now U.S. Patent No. 6,502,135 ("the '135 patent"). The '135 patent is a CIP application of U.S. Patent Application No. 09/429,643, filed October 29, 1999, now U.S. Patent No. 7,010,604 ("the '604 patent"). The '604 patent attempts to claim priority from Provisional Application No. 60/137,704, filed June 7, 1999, and Provisional Application No. 60/106,261, filed October 30, 1998. However, the effective filing date for the embodiments claimed in claims 1 - 41 of the '180 patent is no earlier than April 26, 2000, as explained below.

The '180 patent recites subject matter directed to a method for accessing a secure network address via a secure domain name service, the independent claims are styled as a method, a computer-readable storage medium (comprising instructions for a method for accessing a secure computer network), and a data processing apparatus (which include a memory storing instructions for a method for accessing a secure computer network address). The methodology recited in all three of the independent claims include the steps of receiving a secure domain name, sending a query message, receiving a response message, and sending an message requesting access to the secure network address. For example, independent claim 1 recites:

> 1. A method for accessing a secure computer network address, comprising steps of:
> receiving a secure domain name;
> sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;
> receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and
> sending an access request message to the secure computer network address using

a virtual private network communication link.

independent claim 17 recites:

> 17. A computer-readable storage medium, comprising:
> a storage area; and
> computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:
> receiving a secure domain name;
> sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain name;
> receiving from the domain name service a response message containing the secure computer network address corresponding to the secure domain name; and
> sending an access request message to the secure computer network address using a virtual private network communication link.

and independent claim 33 recites:

> 33. A data processing apparatus, comprising:
> a processor, and
> memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:
> receiving a secure domain name;
> sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;
> receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and
> sending an access request message to the secure computer network address using a virtual private network communication link.

To the extent there is allegedly any written description support, such written descriptive support for this claimed subject matter first appeared in the '209 CIP application, which was filed April 26, 2000, and of which the '180 is a continuation and shares the same specification, including the figures. For example, see the '180 patent at Col. 6, lines 27 - 33, where the '486 application discloses:

> The key technologies provided by the present invention that support the secure virtual Internet include a "one-click" and "no-click" technique to become part of the secure

Petitioner Apple Inc. - Exhibit 1002, p. 427

> virtual Internet, a secure domain name service (SDNS) for the secure virtual Internet, and a new approach for interfacing specific client applications onto the secure virtual Internet.

The same disclosure can be found in the originally-filed specification of the '209 parent application at page 10, lines 22 - 26. Col. 7, lines 31 - 39 of the '486 application and page 11, lines 16 - 22 of the '209 application disclose:

> The advantages of the present invention are provided by a secure domain name service for a computer network that includes a portal connected to a computer network, such as the Internet, and a domain name database connected to the computer network through the portal. According to the invention, the portal authenticates a query for a secure computer network address, and the domain name database stores secure computer network addresses for the computer network.

These portions of the Summary of the Invention were added with the April 26, 2000 filing of the '209 application. Similarly, new material was added on April 26, 2000, beginning at Col. 49, line 54 of the '486 application and page 81, line 15 of the '209 application, where the heading "One-Click Secure On-line Communications and Secure Domain Name Service" first appears.

Further in the '486 and '209 applications, there are disclosed the steps of "querying a secure domain name service" ('486 at Col. 51, line 34 and '209 at page 84, line 8), "Returning to FIG. 34, in step 3410, SDNS 3313 returns a secure URL to software module 3309 for the 'scom address for secure server 3320 corresponding to server 3304" ('486 at Col. 52, lines 38 - 40 and '209 at page 86, lines 1 - 3), and "At step 3411, software module 3309 accesses secure server 3320 through VPN communication link 3321 based on the VPN resources allocated by VPN gatekeeper 3314" ('486 at Col. 52, lines 55 - 57 and '209 at page 86, lines 14 - 16).

None of the four earlier filed applications from which priority is claimed by the '209 parent application includes these exemplary descriptions. Nor is there any other description in the four earlier applications for the claimed subject matter of the '180 patent. Accordingly, prior art as regards independent claims 1, 17, and 33 and, by dependency, claims 4, 10, 12-15, 20, 26, 28-31, and 35 would be any and all documents published before April 26, 2000, and patents with an effective filing date before April 26, 2000.

Petitioner Apple Inc. - Exhibit 1002, p. 428

B. Prosecution History

Claims directed to the approximate or similar subject matter of issued claims 1 - 41 of the '180 patent were first filed on April 26, 2000 as claims 31 - 52 (claim 41 was omitted in the '209 application, and two claim 42's were filed) in the '209 parent application. Similarities can be found between issued '180 patent claims 1 and 17 and claim 31 and the second claim 42, respectively, of the '209 patent. Following a July 3, 2003 restriction requirement in the '209 parent application and an August 4, 2003 election by the Applicants of the '209 application, only claims 1 - 30 remained pending in the '209 application. A Notice of Allowance and a Notice of Allowability were mailed August 12, 2003, with no art rejection having been made by the Examiner. The issue fee for the '209 application was not paid, and a Notice of Abandonment was mailed December 23, 2003.

The '486 application was filed November 7, 2003, as a divisional of the '209 application, with the claims 1 - 24. Originally filed claims 1 - 22 of the '486 application matched claims 31 - 52 of the '209 application. A first Office Action was mailed May 19, 2006 in the '486 application, rejecting independent claims 1 and 12 under 35 U.S.C. § 112, second paragraph, and objecting to claims 2 - 11 and 13 - 24 as depending from a rejected base claim. An amendment in the '486 application was filed August 17, 2006, amending independent claims 1 and 12 by adding "from the secure domain name service" to the sending and the second receiving steps, and adding claims 25 - 41. A Notice of Allowance and a Notice of Allowability were mailed November 21, 2006, allowing all pending claims 1 - 41. No art rejection was ever made in the application. The Notice of Allowability included an Examiner's Statement of Reasons for Allowance:

> The prior arts of record do not teach a system and a method for accessing a secure computer network address comprising steps of: requesting a secure computer network address from a secure domain name server according to the secure domain name; and using a virtual private network communication link to send an access request message to the secure computer network address.

The issue fee was paid January 16, 2007, and the '486 application proceeded to issue.

Petitioner Apple Inc. - Exhibit 1002, p. 429

V. Explanation of the Pertinency and Manner of Applying Newly Cited Prior Art to Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of the '180 Patent, for Which Reexamination is Requested

SNQ #1 **Claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 are unpatentable under 35 USC § 102 (a) for being anticipated by Aventail**

1. Substantial New Question of Patentability

Aventail's disclosure of requesting a secure computer network address from a secure domain name server according to the secure domain name and using a virtual private network communication link to send an access request message to the secure computer network address presents a new, non-cumulative technical teaching that was not previously considered and discussed on the record during prosecution of the '180 patent application (*i.e.*, the Aventail teaching is "new"). In particular, it is submitted that, based on the Examiner's statement of reasons for allowance, the claims of the '180 patent application were allowed because the references of record allegedly lacked requesting a secure computer network address from a secure domain name server according to the secure domain name, which is an element recited in independent claims 1, 17, and 33. As discussed below, Aventail discloses each of these claimed elements and more.

2. Brief Description of the Prior Art

Aventail discusses methods and systems for establishing a virtual private network ("VPN") across a network such as the Internet. Specifically, the reference discloses three main methods for creating a VPN according to Aventail: (1) a basic embodiment where the VPN determination is made at the client computer (p. 8), (2) a proxy chaining embodiment where the VPN determination is made at a proxy server (pp. 68, 72), and (3) a multiproxy embodiment where the VPN determination is made at both the client computer and successive proxy servers (pp. 68-71).

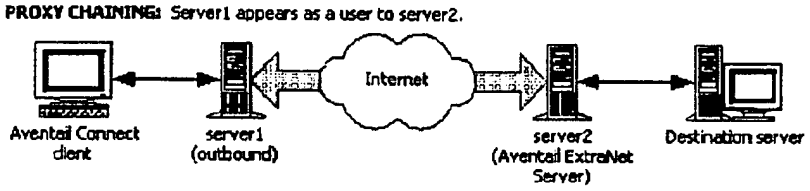
In the basic method, the process begins with the client computer requesting a domain name service (DNS) lookup of a hostname. (p. 8). Aventail Connect, a software program, intercepts the lookup request and determines whether the hostname corresponds to an entry in a list of hostnames maintained by Aventail Connect. If it does not correspond to an entry in the list, Aventail Connect permits the lookup to proceed as if Aventail Connection were not there –

Petitioner Apple Inc. - Exhibit 1002, p. 430

i.e., a typical DNS resolution process. (p. 8). If the hostname is on the list, Aventail Connect recognizes that the hostname requires a VPN and initiates the VPN process according to Aventail. (p. 12). The entire process is transparent to the user, and the VPN according to Aventail is set up automatically based on the DNS lookup request issued by the client computer. (p. 12-13).

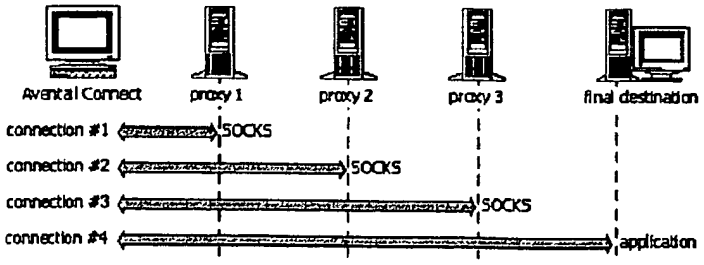
In the proxy chaining method, the functionalities of Aventail Connect are moved to a proxy server (p. 68 – "where one Aventail Extranet server acts as a client to another Aventail Extranet Server"). In other words, when the client computer requests a DNS lookup, the proxy server intercepts the lookup request and makes the determination whether the request is for a destination requiring a VPN connection according to Aventail.

Aventail Connect 3.1/2.6 Admin Guide Page 72:



In the multiproxy method, Aventail Connect at the client computer makes an initial determination that a VPN according to Aventail is required in the same manner as the basic method. Where the process differs, however, is that Aventail Connect must negotiate with successive proxy servers to establish the VPN. (p. 69). Each successive proxy server has its own access and control rules for passing Aventail Client onto the next proxy server. (p. 68).

Aventail Connect 3.1/2.6 Admin Guide Page 69:



Petitioner Apple Inc. - Exhibit 1002, p. 431

In each method, the entire process is transparent to the user and the VPN according Aventail is set up automatically. (p. 12-13).

3. Application of the Prior Art

Independent claim 1 is directed to a method for accessing a secure computer network address, comprising the steps of receiving a secure domain name; sending a query message to a secure domain name service for the corresponding network address; receiving a response message from the secure domain name service containing the network address; and sending an access request message to the secure computer network address using a VPN communication link. In particular, claim 1 recites:

> 1. A method for accessing a secure computer network address, comprising steps of:
> receiving a secure domain name;
> sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;
> receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and
> sending an access request message to the secure computer network address using a virtual private network communication link.

Each of the steps of claim 1 is disclosed in the Aventail Administrator's Guide, which published no later than 1999, before the April 26, 2000 filing of the '209 CIP patent application. As discussed above, the disclosure of the '180 patent that provides written descriptive support, if any, of the claims of the '180 patent was introduced to the specification with the April 26, 2000 filing of the '209 parent CIP application filing. As such, the 1999 Aventail Administrator's Guide is prior art to the '180 patent claims. A claim chart showing exemplary description of each of the limitations recited in claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 of the '180 patent as found in Aventail is attached hereto as Appendix A.

The preamble of claim 1 requires "a method for accessing a secure computer network address." Aventail discloses such a feature at pages 46 and 79. Aventail creates SOCKS 5 connections for authenticated firewall traversal. According to the Court in the Litigation, a "secure computer network address" means "a network address that requires authorization for access and is associated with a computer capable of virtual private network communications." Exhibit 13 at page 28. Aventail at pages 12 and 46 discloses that authentication may be required

Petitioner Apple Inc. - Exhibit 1002, p. 432

before access is granted to resources at the remote service.

Throughout this Request, Requester will reference the Court's July 30, 2009 claim constructions, included herein as Exhibit 13. This is not an admission that Requester agrees with the Court's constructions. The Requester is simply illustrating that the prior art references, even under the Court's constructions, anticipate and/or render obvious the claims of the '180 patent.

Claim 1 further requires, "receiving a secure domain name." According to the Court in the Litigation, a "secure domain name" means "a domain name that corresponds to a secure computer network address." Exhibit 13 at page 30. Aventail discloses a domain name service for resolving domain names to IP addresses. See pages 11 and 12. Aventail Connect (the software at the client computer) receives a domain name from the user. The domain name is a secure domain name because it corresponds to a computer with an Aventail VPN connection that requires authentication before it can be accessed.

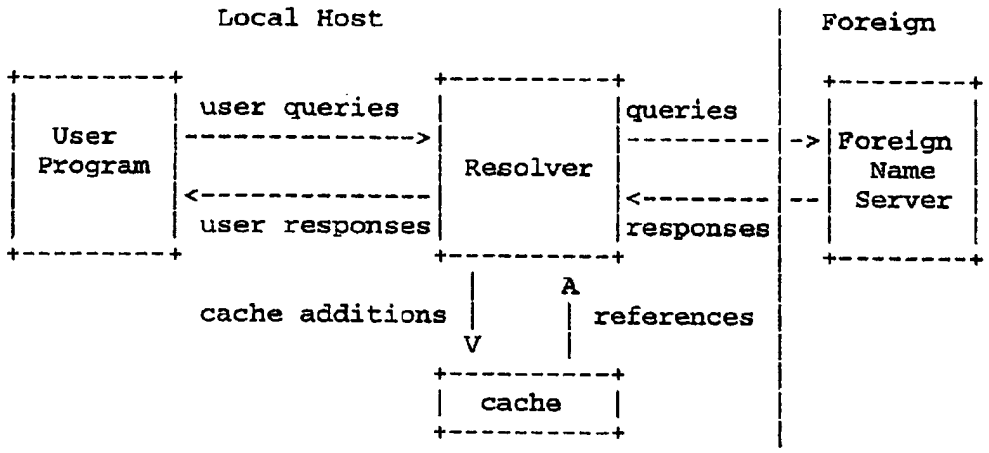
Claim 1 then requires "sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name." The Court in the Litigation construes "secure domain name service" broadly to include "a lookup service that returns a secure network address for a requested secure domain name." Exhibit 12 at page 32. Accordingly, a "secure domain name service" includes any lookup service that resolves a secure domain name.

There are two "lookup services" described in Aventail that independently satisfy this limitation. The first "lookup service" is a lookup service at the client computer. See page 8, which discusses a local DNS lookup. The alternative "lookup service" disclosed in Aventail is a more traditional DNS server that is located away from the client. See page 12, where the domain name is sent to the SOCKS server for resolution. In both cases, the domain name services are secure domain name services because they resolve the secure domain name to a corresponding secure computer network address.

The next limitation of claim 1 requires, "receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name." As discussed above, there are two "lookup services" disclosed in Aventail that independently satisfy the secure domain name service limitation. In both cases, the domain name is resolved to an IP address that is passed back to the client computer. See page 12, which discusses an "IP address provided by the application." This is corroborated by RFC 1035, the

Petitioner Apple Inc. - Exhibit 1002, p. 433

standard for Internet domain name resolution, at least at page 4.



The final limitation of claim 1 requires, "sending an access request message to the secure computer network address using a virtual private network communication link." Aventail discloses such a feature at page 8. A VPN according to Aventail is established so that the client computer can securely access resources using a public network. As introduced above, the subject matter recited in claim 1 of the '180 patent is fully disclosed in Aventail.

Claims 4, 10, and 12-15 depend directly or ultimately from claim 1 and include further limitations that are disclosed in the Aventail Administrator's Guide, as shown in Appendix A. In brief illustration of select claims (Appendix A provides details for every claim):

For example, claim 4 recites that the response message contains provisioning information for the virtual private network. While the '180 patent does not expressly disclose "provisioning information," Aventail , at least at pages 68, 69, and 77, discloses that Aventail Connect provides link, authentication, and access control information to allow secure access to a final destination across multiple firewalls of a network.

Claim 10 recites that the virtual private network includes the Internet, which Aventail discloses at pages 5, 8, and 79.

Claim 12 recites the access request message contains a request for information stored at the secure computer network address. This feature is disclosed in Aventail at least at pages 8 and 69.

Claim 14 recites that the method of claim 1 (see above) is performed by a software

Petitioner Apple Inc. - Exhibit 1002, p. 434

module, and claim 15 recites that the method of claim 1 is performed by a client computer. Aventail is installed at the client computer and performs the method of claim 1. Aventail receives the secure domain name at the client computer, sends the name for resolution, receives the IP address, and issues the access request to the secure computer network address. See claim 1. As introduced above, the subject matter recited in claims 14 and 15 of the '180 patent is fully disclosed in Aventail.

Accordingly, for these reasons, for the reasons discussed above regarding claim 1, and based upon the citations presented in Appendix A, it is respectfully asserted that each of the limitations of claims 4, 10, and 12-15 is fully disclosed in Aventail, which therefore anticipates each of claims 4, 10, and 12-15.

Independent claim 17 is directed to subject matter similar to that recited in claim 1, except that claim 17 is styled as a computer-readable storage medium comprising a storage area and computer-readable instructions for performing the steps recited in claim 1. In particular, claim 17 recites:

> 17. A computer-readable storage medium, comprising:
> a storage area; and
> computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:
> receiving a secure domain name;
> sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain name;
> receiving from the domain name service a response message containing the secure computer network address corresponding to the secure domain name; and
> sending an access request message to the secure computer network address using a virtual private network communication link.

As discussed above regarding claim 1, the Aventail Administrator's Guide discloses each of the limitations of claim 17 that recite subject matter similar to that of claim 1. Further, Aventail discloses that the program code for Aventail is available by CD or can be delivered by network - i.e., computer readable instructions. See Aventail at page 14. Such computer code would be installed into a storage area at the client. Accordingly, Aventail fully anticipates the limitations of claim 17.

Claims 20, 26, and 28 - 31 depend directly or ultimately from claim 17 and include

Petitioner Apple Inc. - Exhibit 1002, p. 435

further limitations that are disclosed in Aventail, as shown in Appendix A. The limitations recited in claims 20, 26, and 28 - 31 map closely to the limitations recited in claims 4, 10, and 12-15, respectively. Accordingly, for this reason, for the reasons discussed above regarding claim 17, for the reasons discussed above regarding claims 1, 4, 10, and 12-15, and based on the citations presented in Appendix A, it is respectfully asserted that each of the limitations of claims 20, 26, and 28 - 31 is fully disclosed in Aventail, which therefore anticipates each of claims 20, 26, and 28 - 31.

Independent claim 33 is directed to subject matter similar to that recited in claim 1, except that claim 33 is styled as a data processing apparatus comprising a processor and memory storing instructions for performing the steps recited in claim 1. In particular, claim 33 recites:

> 33. A data processing apparatus, comprising:
> a processor, and
> memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:
> receiving a secure domain name;
> sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;
> receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and
> sending an access request message to the secure computer network address using a virtual private network communication link.

As discussed above regarding claim 1, Aventail discloses each of the limitations of claim 33 that recite subject matter similar to that of claim 1. Further, Aventail discloses the well-known data processing apparatus and processors in conjunction with the use of computers across networks, including the Internet. See Aventail at pages 7, 8, 13, and 72. Accordingly, Aventail fully anticipates the limitations of claim 33.

Claim 35 depends directly or ultimately from claim 33 and includes further limitations that are disclosed in Aventail, as shown in Appendix A. The limitations recited in claim 35 map closely to the limitations recited in claim 4. Accordingly, for this reason, for the reasons discussed above regarding claim 33, for the reasons discussed above regarding claim 4, and based on the citations presented in Appendix A, it is respectfully asserted that each of the

Petitioner Apple Inc. - Exhibit 1002, p. 436

limitations of claim 35 is fully disclosed in Aventail, which therefore anticipates claim 35.

For the reasons presented above, it is respectfully submitted that each of claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 of the '180 patent is fully disclosed, and therefore anticipated under 35 U.S.C. § 102(a), by the Aventail Administrator's Guide prior art reference.

SNQ #2 **Claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 are unpatentable under 35 USC § 103(a) for being obvious over VPN Overview in view of RFC 1035**

1. Substantial New Question of Patentability

VPN Overview/RFC 1035's disclosure of requesting a secure computer network address from a secure domain name server according to the secure domain name and using a virtual private network communication link to send an access request message to the secure computer network address presents a new, non-cumulative technical teaching that was not previously considered and discussed on the record during prosecution of the '180 patent application (*i.e.*, the VPN Overview and RFC 1035 teachings are "new"). In particular, it is submitted that, based on the Examiner's statement of reasons for allowance, the claims of the '180 patent application were allowed because the references of record allegedly lacked requesting a secure computer network address from a secure domain name server according to the secure domain name, which is an element recited in independent claims 1, 17, and 33. As discussed below, the VPN Overview/RFC 1035 combination discloses each of these claimed elements and more.

2. Brief Description of the Prior Art

VPN Overview is another prior art reference that discusses the PPTP feature offered by Windows NT 4.0, prior to the filing date of the '180 patent. In addition to PPTP, VPN Overview further discloses the use of L2TP and IPsec for creating virtual private networks across the Internet. Connection requests for a secured domain name arrive at, for example, a VPN tunnel server, which resolves addresses against the Windows NT Domain Controller. (p. 27) Once resolved, the local resource's credentials are authenticated and a virtual private network is automatically created between the local resource and the remote resource. (p. 22).

Petitioner Apple Inc. - Exhibit 1002, p. 437

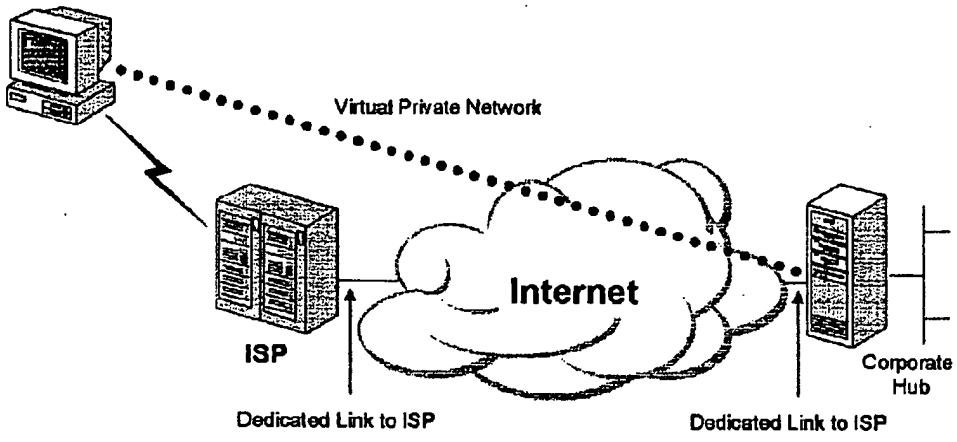
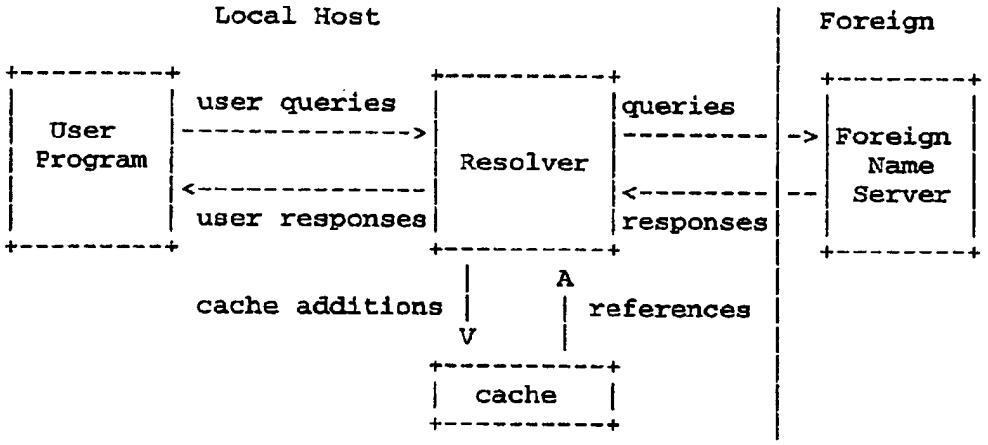


Figure 2: Using a VPN to connect a remote client to a private LAN

RFC 1035 specifies the standard for domain name resolution of Internet domain names. Upon receiving a domain name, the client computer passes the domain name to a resolver or name server to resolve the domain name to an IP address. Once resolved, the IP address is passed back to the requesting computer, which can then make a connection to the IP address. See RFC 1035 at page 4:



3. Application of the Prior Art

As discussed above in Section V(SNQ #1), independent claim 1 is directed to a method for accessing a secure computer network address, comprising the steps of receiving a secure

Petitioner Apple Inc. - Exhibit 1002, p. 438

domain name; sending a query message to a secure domain name service for the corresponding network address; receiving a response message from the secure domain name service containing the network address; and sending an access request message to the secure computer network address using a VPN communication link.

Each of the steps of claim 1 is disclosed in the VPN Overview reference or the RFC 1035 reference, which were respectively published in 1998 and 1987, before the April 26, 2000 filing of the '209 CIP patent application. As discussed above, the disclosure of the '180 patent that provides written descriptive support, if any, of the claims of the '180 patent was introduced to the specification with the April 26, 2000 filing of the '209 parent CIP application. As such, the VPN Overview reference, which was published in 1998; and the RFC 1035 reference, which was published in 1987, are both prior art to the '180 patent claims. A claim chart showing exemplary description of each of the limitations recited in claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 of the '180 patent as found in the VPN Overview and the RFC 1035 references is attached hereto as Appendix B.

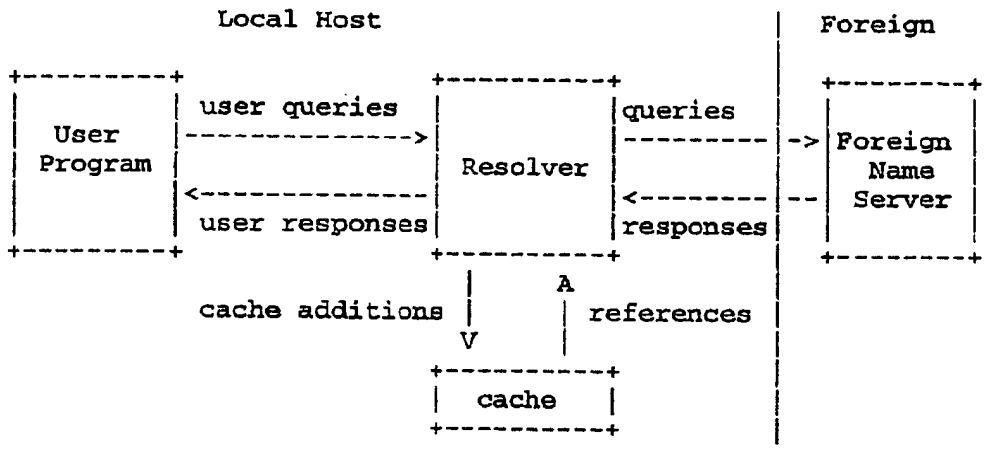
The preamble of claim 1 requires "a method for accessing a secure computer network address." VPN Overview discloses such a feature at page 6. According to the Court in the Litigation, a "secure computer network address" means "a network address that requires authorization for access and is associated with a computer capable of virtual private network communications." Exhibit 13 at page 28. VPN Overview discloses at page 9 that authentication may be required before access is granted to resources at the remote service.

Claim 1 further requires, "receiving a secure domain name." According to the Court in the Litigation, a "secure domain name" means "a domain name that corresponds to a secure computer network address." Exhibit 13 at page 30. VPN tunnel servers can be identified using domain names. See page 26, which illustrates that a VPN tunnel server can be named "vpnx.support.bigcompany.com." This name corresponds to a secure network address – i.e., the address require authorization. The client computer receives this domain name from the user when the user identifies to where the VPN connection is to be made.

Claim 1 then requires "sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name." The Court in the Litigation construes "secure domain name service" broadly to include "a lookup service that returns a secure network

address for a requested secure domain name." Exhibit 13 at page 32. Accordingly, a "secure domain name service" includes any lookup service that resolves a secure domain name.

As mentioned previously, VPN Overview discloses that VPN tunnel servers may be identified using domain names. There is further disclosure in VPN Overview at pages 6 and 7 discussing connections made over the Internet. RFC 1035 teaches that, in order to make a connection to an Internet domain name, the domain name is sent to a domain name service for resolution and then passed back the IP address. RFC 1035 at page 4:



Accordingly, RFC 1035 discloses the limitation.

The next limitation of claim 1 requires, "receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name." RFC 1035 discloses at page 4 that the domain name is resolved and passed back as part of the user response.

The final limitation of claim 1 requires, "sending an access request message to the secure computer network address using a virtual private network communication link." See VPN Overview at pages 6 - 10, 12, 14, 22, and 26 - 28. The purpose of the VPN is to access information at the VPN tunnel server using a VPN communication link. As introduced above, the subject matter recited in claim 1 of the '180 patent is fully disclosed in VPN Overview and RFC 1035.

Claims 4, 10, and 12 - 15 depend directly or ultimately from claim 1 and include further limitations that are disclosed in the VPN Overview or the RFC 1035 references, as shown in

Petitioner Apple Inc. - Exhibit 1002, p. 440

Appendix B. In brief illustration of select claims (Appendix B provides details for every claim):

Claim 4 recites that the response message contains provisioning information for the virtual private network. VPN Overview, at least at pages 9, 26, and 27, discloses this feature. Information is exchanged between the computers to set up the VPN.

Claim 10 recites the virtual private network includes the Internet, which is disclosed in the VPN Overview reference at least at page 6.

Claim 12 recites that the access request message contains a request for information stored at the secure computer network address. This feature is disclosed in VPN Overview at least at pages 6 and 7. For example, VPN Overview describes that one use of the VPN is to permit users to work remotely – i.e., use resources at the corporate site while at home or on the road.

Claim 14 recites that the method of claim 1 (see above) is performed by a software module, and claim 15 recites that the method of claim 1 is performed by a client computer. VPN Overview discloses a method for accessing a secure computer network address across a virtual private network. See VPN Overview at page 6 and as in Appendix B. VPN Overview also discloses receiving at a software module (i.e., Windows NT client) on a client computer a domain name for a secure remote computer and sending the domain name to a Domain Name System server for requesting a secure IP address corresponding to the domain name. See VPN Overview at pages 6, 7, and 26 - 27. VPN Overview discloses the use of DNS. As outlined in RFC 1035, DNS includes returning the IP address to the client computer. See RFC 1035 at least at pages 3, 4, and 20 - 21. Finally, a request is made from the software module at the client computer to connect to the specified remote computer via a secure virtual private network. See VPN Overview at pages 6 - 10, 12, 14, 22, and 26 - 28. As introduced above, the subject matter recited in claims 14 and 15 of the '180 patent is fully disclosed in the VPN Overview and RFC 1035 references.

Accordingly, for these reasons, for the reasons discussed above regarding claim 1, and based upon the citations presented in Appendix B, it is respectfully asserted that each of the limitations of claims 4, 10, and 12 - 15 is fully disclosed in the VPN Overview or RFC 1035 references.

As also discussed above in Section V(SNQ #1), independent claim 17 is directed to subject matter similar to that recited in claim 1, except that claim 17 is styled as a computer-

Petitioner Apple Inc. - Exhibit 1002, p. 441

readable storage medium comprising a storage area and computer-readable instructions for performing the steps recited in claim 1. As discussed above regarding claim 1, the VPN Overview/RFC 1035 combination discloses each of the limitations of claim 17 that recite subject matter similar to that of claim 1. VPN Overview, furthermore, discloses the well-known use of computer memory to store information, at least at pages 10 and 21. Computer-readable instructions are well-known parts of computer software application programs, which the systems described in VPN Overview are using. See VPN Overview at pages 10 and 21. Accordingly, the VPN Overview/RFC 1035 combination fully discloses the limitations of claim 17.

Claims 20, 26, and 28 - 31 depend directly or ultimately from claim 17 and include further limitations that are disclosed in the VPN Overview and RFC 1035 references, as shown in Appendix B. The limitations recited in claims 20, 26, and 28 - 31 map closely to the limitations recited in claims 4, 10, and 12 - 15, respectively. Accordingly, for this reason, for the reasons discussed above regarding claim 17, for the reasons discussed above regarding claims 4, 10, and 12 - 15, and based upon the citations presented in Appendix B, it is respectfully asserted that each of the limitations of claims 20, 26, and 28 - 31 is fully disclosed in the VPN Overview and RFC 1035 references, which therefore render each of claims 20, 26, and 28 - 31 obvious.

As also discussed above in Section V(SNQ #1), independent claim 33 is directed to subject matter similar to that recited in claim 1, except that claim 33 is styled as a data processing apparatus comprising a processor and memory storing instructions for performing the steps recited in claim 1. As discussed above regarding claim 1, the VPN Overview/RFC 1035 combination discloses each of the limitations of claim 33 that recite subject matter similar to that of claim 1. Further, VPN Overview discloses the well-known data processing apparatus and processors in conjunction with the use of computers across networks, including the Internet. See VPN Overview at pages 10 and 21. Accordingly, the VPN Overview/RFC 1035 combination renders claim 33 obvious.

Claim 35 depends directly from claim 33 and includes further limitations that are disclosed in the VPN Overview or RFC 1035 references, as shown in Appendix B. The limitations recited in claim 35 maps closely to the limitations recited in claim 4. Accordingly, for this reason, for the reasons discussed above regarding claim 33, for the reasons discussed above regarding claims 4, and based upon the citations presented in Appendix B, it is respectfully asserted that each of the limitations of claim 35 is fully disclosed in the VPN

Petitioner Apple Inc. - Exhibit 1002, p. 442

Overview and RFC 1035 references, which therefore render claim 35 obvious.

There are several reasons to combine the VPN Overview and RFC 1035 references in the manner discussed above to render claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 obvious. *KSR Int'l v. Teleflex, Inc.*, 127 S.Ct. 1727, 1733, 1743-44. A person of ordinary skill in the art of secure network communication, at the time the '180 patent was filed, and in possession of the VPN Overview reference would want to know the protocol and technique for obtaining the network address through the domain name service should a domain name be available. The RFC 1035 document, published more than ten years before both the publication of the VPN Overview reference and the filing of the '180 patent, would provide this sought-after information. It would only make sense for this skilled artisan to have drawn on the RFC 1035 protocols for obtaining the IP address of the domain name and returning it to the user in response to the query. By doing so, the artisan would be taking advantage of known methodologies for obtaining the network address to communicate with the requested domain.

For the reasons presented above, it is respectfully submitted that each of claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 of the '180 patent is fully disclosed, and therefore obvious under 35 U.S.C. § 103(a) by the VPN Overview and RFC 1035 references.

SNQ #3 **Claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 are unpatentable under 35 USC § 102(b) for being anticipated by Kosiur**

1. Substantial New Question of Patentability

Kosiur's disclosure of requesting a secure computer network address from a secure domain name server according to the secure domain name and using a virtual private network communication link to send an access request message to the secure computer network address presents a new, non-cumulative technical teaching that was not previously considered and discussed on the record during prosecution of the '180 patent application (*i.e.*, the Kosiur teaching is "new"). In particular, it is submitted that, based on the Examiner's statement of reasons for allowance, the claims of the '180 patent application were allowed because the references of record allegedly lacked requesting a secure computer network address from a secure domain name server according to the secure domain name, which is an element recited in independent claims 1, 17, and 33. As discussed below, Kosiur discloses each of these claimed elements and more.

Petitioner Apple Inc. - Exhibit 1002, p. 443

2. Brief Description of the Prior Art

Kosiur describes the building, operation, and management of virtual private networks over the Internet. Pages 37 and 40-42. Virtual private networks are created by establishing a "tunnel" through the Internet between two resources:

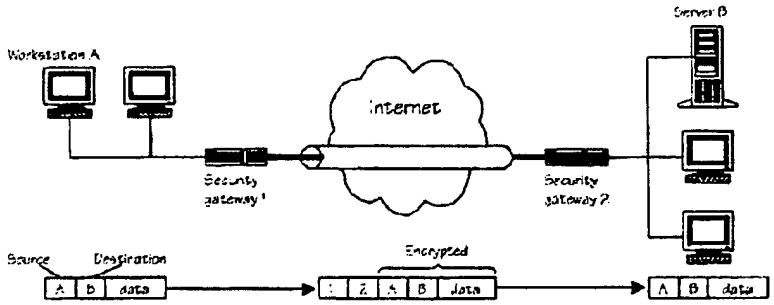


FIGURE 3.2 Schematic of a tunnel.

Tunnels can be established in several different ways. In relevant part to the '180 patent, Kosiur acknowledges that VPNs often use DNS servers to resolve connection requests. Page 36.

For example, a corporation may keep an internal DNS server for resolving VPN requests behind a firewall and a second VPN DNS server outside the firewall. (p. 296). When a connection request for a secured resource outside the firewall is made, the internal VPN DNS server forwards the connection request to the external DNS server. (p. 296). The domain name is resolved and the external DNS server negotiates the connection request and establishes a VPN between the local and remote sources. (p. 47, 297).

3. Application of the Prior Art

As discussed above in Section V(SNQ #1), independent claim 1 is directed to a method for accessing a secure computer network address, comprising the steps of receiving a secure domain name; sending a query message to a secure domain name service for the corresponding network address; receiving a response message from the secure domain name service containing the network address; and sending an access request message to the secure computer network address using a VPN communication link.

Each of the steps of claim 1 is disclosed in Kosiur, which was published in 1998, before the April 26, 2000 filing of the '209 CIP patent application. As discussed above, the disclosure

Petitioner Apple Inc. - Exhibit 1002, p. 444

of the '180 patent that provides written descriptive support, if any, of the claims of the '180 patent was introduced to the specification with the April 26, 2000 filing of the '209 parent CIP application. As such, the 1998 Kosiur is prior art to the '180 patent claims. A claim chart showing exemplary description of each of the limitations recited in claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 of the '180 patent as found in the Kosiur is attached hereto as Appendix C.

The preamble of claim 1 requires "a method for accessing a secure computer network address." Kosiur discloses such a feature at pages 37 and 41-42, which discuss the use of a VPN to secure communications across a network such as the Internet. According to the Court in the Litigation, a "secure computer network address" means "a network address that requires authorization for access and is associated with a computer capable of virtual private network communications." Exhibit 13 at page 28. Kosiur disclose at pages 47 and 132 that authentication may be required before access is granted to resources at the remote service.

Claim 1 further requires, "receiving a secure domain name." According to the Court in the Litigation, a "secure domain name" means "a domain name that corresponds to a secure computer network address." Exhibit 13 at page 30. Kosiur is replete with references to domain name usage with VPN enabled servers and computers. See, for example, pages 293-296. These domain names are "secure" according to the Court's construction because the domain names correspond to network addresses that require authentication. These names are received at the client computer from a user attempting to reach the named site.

Claim 1 then requires "sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name." The Court in the Litigation construes "secure domain name service" broadly to include "a lookup service that returns a secure network address for a requested secure domain name." Exhibit 13 at page 32. Accordingly, a "secure domain name service" includes any lookup service that resolves a secure domain name.

As mentioned in a previous paragraph, Kosiur discloses Internet domain names for identifying VPN resources. When a user enters a domain name at the client computer, the client computer issues a lookup request to a domain name service server. See pages 293-296.

The next limitation of claim 1 requires, "receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure

Petitioner Apple Inc. - Exhibit 1002, p. 445

domain name." Kosiur discloses at pages 293-296 that domain name resolution occurs at DNS servers. The DNS servers pass back the corresponding network address.

The final limitation of claim 1 requires, "sending an access request message to the secure computer network address using a virtual private network communication link." See Kosiur at pages 40-42. The purpose of the VPN is to access information across a network connection, which requires sending an access request message over the established VPN link to the IP address at the far end. As introduced above, the subject matter recited in claim 1 of the '180 patent is fully disclosed in Kosiur.

Claims 4, 10, and 12 - 15 depend directly or ultimately from claim 1 and include further limitations that are disclosed in Kosiur, as shown in Appendix C. In brief illustration of select claims (Appendix C provides details for every claim):

Claim 4 recites that the response message contains provisioning information for the virtual private network. Kosiur, at least at pages 40 - 42, 132, 296, 308 - 309, and 311, discloses the RSVP feature for providing information for allocating and reserving network resources and paths for the network.

Claim 10 recites the virtual private network includes the Internet, which is disclosed in Kosiur at least at page 379.

Claim 12 recites that the access request message contains a request for information stored at the secure computer network address. Kosiur discloses at least at pages 40 – 42, 133, and 276 - 277 the feature of requesting data or requesting authentication information to establish a secure link.

Claims 14 and 15 recite that the method of claim 1 is performed by a software module and that the method is performed by a client computer. Kosiur discloses a method for accessing a secure computer network address across a virtual private network. See Kosiur at pages 37, 40 - 42, and 379 and as in Appendix C. Kosiur discloses receiving at a software module (i.e., Windows NT client or server – depending on which computer is acting as the "client") on a client computer a domain name for a secure destination computer and sending the domain name to a Domain Name Service server for converting the domain name into a secure IP address. See Kosiur at pages 216, and 293 - 294. The IP address is returned to the software module at the client computer, and a request is made from the software module to create the secure connection to the specified destination computer. See Kosiur at pages 40 - 42, 47, and 296. As introduced

Petitioner Apple Inc. - Exhibit 1002, p. 446

above, the subject matter recited in claims 14 and 15 of the '180 patent is fully disclosed in the Kosiur reference.

Accordingly, for these reasons, for the reasons discussed above regarding claim 1, and based upon the citations presented in Appendix C, it is respectfully asserted that each of the limitations of claims 4, 10, and 12 - 15 is fully disclosed in Kosiur, which therefore anticipates each of claims 4, 10, and 12 - 15.

As also discussed above in Section V(SNQ #1), independent claim 17 is directed to subject matter similar to that recited in claim 1, except that claim 17 is styled as a computer-readable storage medium comprising a storage area and computer-readable instructions for performing the steps recited in claim 1. As discussed above regarding claim 1, Kosiur discloses each of the limitations of claim 17 that recite subject matter similar to that of claim 1. Further, Kosiur discloses the well-known use of computer memory to store information at least at pages 111 and 162. Computer-readable instructions correspond to the software performing the functions disclosed in the reference. See Kosiur at page 111. Accordingly, Kosiur fully anticipates the limitations of claim 17.

Claims 20, 26 and 28 - 31 depend directly or ultimately from claim 17 and include further limitations that are disclosed in Kosiur, as shown in Appendix C. The limitations recited in claims 20, 26 and 28 - 31 map closely to the limitations recited in claims 4, 10, and 12 - 15, respectively. Accordingly, for this reason, for the reasons discussed above regarding claim 17, for the reasons discussed above regarding claims 4, 10, and 12 - 15, and based upon the citations presented in Appendix C, it is respectfully asserted that each of the limitations of claims 20, 26 and 28 - 31 is fully disclosed in Kosiur, which therefore anticipates each of claims 20, 26 and 28 - 31.

As also discussed above in Section V(SNQ #1), independent claim 33 is directed to subject matter similar to that recited in claim 1, except that claim 33 is styled as a data processing apparatus comprising a processor and memory storing instructions for performing the steps recited in claim 1. As discussed above regarding claim 1, Kosiur discloses each of the limitations of claim 33 that recite subject matter similar to that of claim 1. Further, Kosiur discloses the well-known data processing apparatus and processors in conjunction with the use of computers across networks, including the Internet. See Kosiur at pages 34, 37, and 40 - 42. Accordingly, Kosiur fully anticipates the limitations of claim 33.

Petitioner Apple Inc. - Exhibit 1002, p. 447

Claim 35 depends directly or ultimately from claim 33 and includes further limitations that are disclosed in Kosiur, as shown in Appendix C. The limitations recited in claim 35 map closely to the limitations recited in claim 4. Accordingly, for this reason, for the reasons discussed above regarding claim 33, for the reasons discussed above regarding claim 4, and based upon the citations presented in Appendix C, it is respectfully asserted that each of the limitations of claim 35 is fully disclosed in Kosiur, which therefore anticipates claims 35. For the reasons presented above, it is respectfully submitted that each of claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 of the '180 patent is fully disclosed, and therefore anticipated under 35 U.S.C. § 102(b), by the Kosiur prior art reference.

SNQ #4 **Claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 are unpatentable under 35 U.S.C. § 102(a) for being anticipated by Kaufman**

1. Substantial New Question of Patentability

Kaufman's disclosure of requesting a secure computer network address from a secure domain name server according to the secure domain name and using a virtual private network communication link to send an access request message to the secure computer network address presents a new, non-cumulative technical teaching that was not previously considered and discussed on the record during prosecution of the '180 patent application (*i.e.*, the Kaufman teaching is "new"). In particular, it is submitted that, based on the Examiner's statement of reasons for allowance, the claims of the '180 patent application were allowed because the references of record allegedly lacked requesting a secure computer network address from a secure domain name server according to the secure domain name, which is an element recited in independent claims 1, 17, and 33. As discussed below, Kaufman discloses each of these claimed elements and more.

2. Brief Description of the Prior Art

Kaufman is a reference disclosing the use of IPsec to secure communications through the Internet using authentication and encryption. IPsec is a framework of standards for helping to ensure private, secure communications by supporting network-level data integrity, data confidentiality, data origination authentication, and replay protection. In relevant part to the '180 patent, Kaufman discloses methods for tunneling through the Internet to create a virtual private

Petitioner Apple Inc. - Exhibit 1002, p. 448

network between two resources. Pages 141-142. These resources can be on the Internet, an intranet, an extranet, or mobile network.

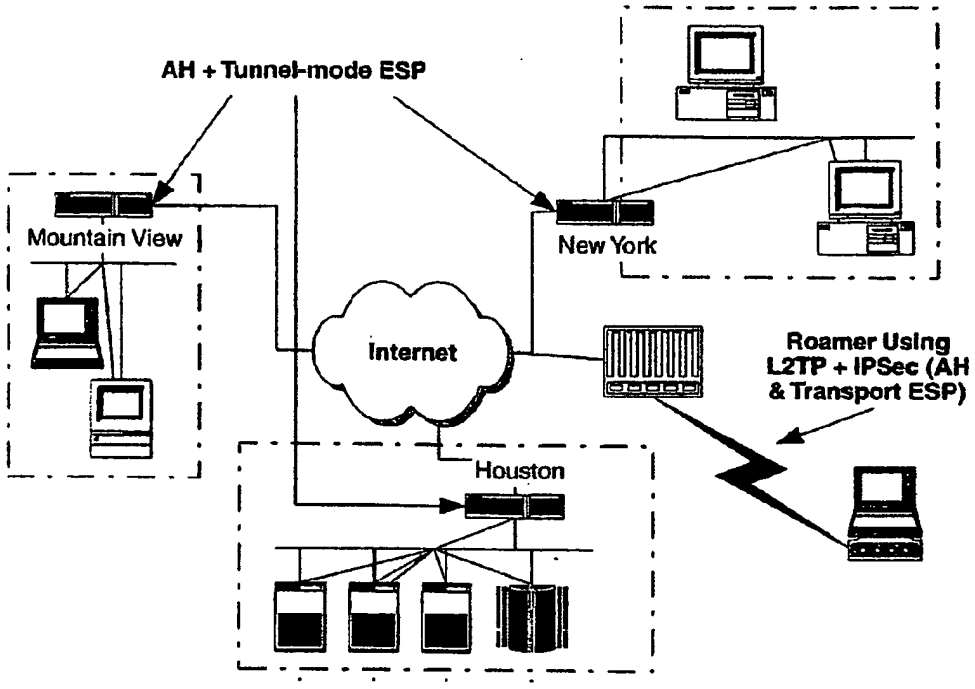


Figure 9.1 IPsec VPN.

In practice, an IPsec connection request over the Internet for a secured resource can use, for example, a DNS server to resolve the request. (p. 127). Once the secured domain name is resolved, a connection can be established between the secured resource and the computer requesting the connection. IPsec includes two basic security protocols: an authentication header and an encapsulating security payload. (p. 78). The secured resource verifies the authenticity of the sender, and a connection is established. (p. 78).

3. Application of the Prior Art

As discussed above in Section V(SNQ #1), independent claim 1 is directed to a method for accessing a secure computer network address, comprising the steps of receiving a secure domain name; sending a query message to a secure domain name service for the corresponding network address; receiving a response message from the secure domain name service containing

Petitioner Apple Inc. - Exhibit 1002, p. 449

the network address; and sending an access request message to the secure computer network address using a VPN communication link.

Each of the steps of claim 1 is disclosed in the Kaufman reference, which was published in 1999, before the April 26, 2000 filing of the '209 CIP patent application. As discussed above, the disclosure of the '180 patent that provides written descriptive support, if any, of the claims of the '180 patent was introduced to the specification with the April 26, 2000 filing of the '209 parent CIP application. As such, the 1999 Kaufman reference is prior art to the '180 patent claims. A claim chart showing exemplary description of each of the limitations recited in claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 of the '180 patent as found in Kaufman is attached hereto as Appendix D.

The preamble of claim 1 requires "a method for accessing a secure computer network address." Kaufman discloses the use of IPsec to create a VPN extranet over the Internet at pages 140-142. According to the Court in the Litigation, a "secure computer network address" means "a network address that requires authorization for access and is associated with a computer capable of virtual private network communications." Exhibit 13 at page 28. Kaufman discloses that IPsec includes several different mechanisms for authenticating users before access is granted to resources at the remote service. See at least pages 2 and 9.

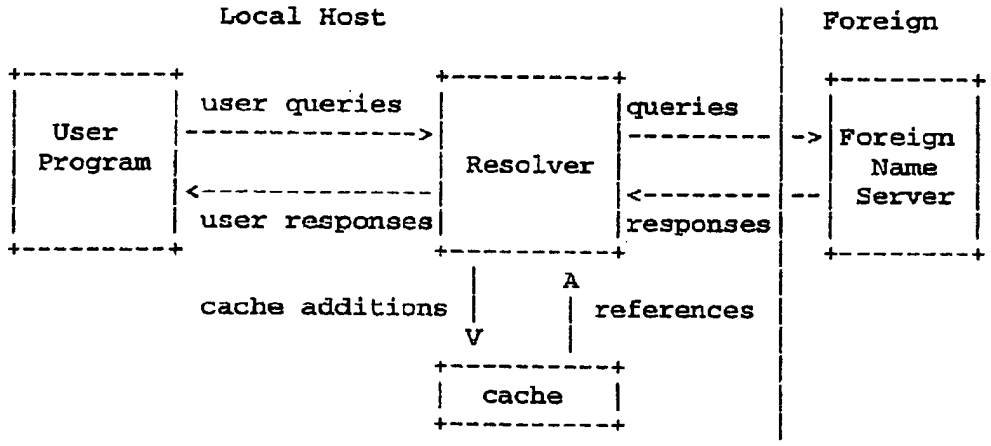
Claim 1 further requires, "receiving a secure domain name." According to the Court in the Litigation, a "secure domain name" means "a domain name that corresponds to a secure computer network address." Exhibit 13 at page 30. As discussed concerning the preamble, Kaufman discloses that IPsec includes secure computer network addresses. Kaufman further discloses that the secure computer network addresses can be referenced using domain names. See page 127. Accordingly such domain names are "secure" domain names under the Court's construction because the domain names correspond to secure computer network addresses. These names are received at the client computer from a user attempting to reach the name.

Claim 1 then requires "sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name." The Court in the Litigation construes "secure domain name service" broadly to include "a lookup service that returns a secure network address for a requested secure domain name." Exhibit 13 at page 32. Accordingly, a "secure domain name service" includes any lookup service that resolves a secure domain name.

Petitioner Apple Inc. - Exhibit 1002, p. 450

As mentioned in a previous paragraph, Kaufman discloses Internet domain names for identifying IPsec resources. When a user enters a domain name at the client computer, the client computer issues a lookup request to a domain name service server to resolve an IP address from a domain name and to enable secure communication over the network. See pages 125, 127, 128, 143 - 144, 191, and 243. Kaufman also discloses the use of DNSSEC as the standards and security mechanisms specific to domain name services. See page 128.

The next limitation of claim 1 requires, "receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name." Kaufman at pages 125, 127, 128, and 191 discuss the use of DNS. In DNS, the resolution server passes back the corresponding network address. RFC 1035 provides corroboration at page 4:



The final limitation of claim 1 requires, "sending an access request message to the secure computer network address using a virtual private network communication link." See Kaufman at pages 140-142. The purpose of the IPsec is to permit the secure access information across a public network connection using a virtual private network. As introduced above, the subject matter recited in claim 1 of the '180 patent is fully disclosed in Kaufman.

Claims 4, 10 and 12 - 15 depend directly or ultimately from claim 1 and include further limitations that are disclosed in Kaufman, as shown in Appendix D. In brief illustration of select claims (Appendix D provides details for every claim):

For example, claim 4 recites that the response message contains provisioning information

Petitioner Apple Inc. - Exhibit 1002, p. 451

for the virtual private network. Kaufman, at least at page 121, discloses this feature.

Claim 10 recites the virtual private network includes the Internet, which is disclosed in Kaufman at least at page 126.

Claim 12 recites that the access request message contains a request for information stored at the secure computer network address. This feature is disclosed in Kaufman at least at pages 141 - 142.

Claims 14 and 15 recite that the method of claim 1 is performed by a software module and that the method is performed by a client computer. Kaufman discloses a method for accessing a secure computer network address across a virtual private network. See Kaufman at pages 140 - 144 and as in Appendix D. Kaufman also discloses receiving a domain name at a software module on a client computer (i.e., IPsec host computer) for a secure destination computer and sending the domain name to a Domain Name System server for resolving the domain name to a secure IP address. See Kaufman at pages 125, 127, 128, 191, and 243. The IP address is returned to the software module at the client computer, and a request is made to begin the secure connection to the specified destination computer. See Kaufman at pages 125, 127, 128, 191, and 243. As introduced above, the subject matter recited in claims 14 and 15 of the '180 patent is fully disclosed in Kaufman.

Accordingly, for these reasons, for the reasons discussed above regarding claim 1, and based upon the citations presented in Appendix D, it is respectfully asserted that each of the limitations of claims 4, 10 and 12 - 15 is fully disclosed in Kaufman, which therefore anticipates each of claims 4, 10 and 12 - 15.

As also discussed above in Section V(SNQ #1), independent claim 17 is directed to subject matter similar to that recited in claim 1, except that claim 17 is styled as a computer-readable storage medium comprising a storage area and computer-readable instructions for performing the steps recited in claim 1. As discussed above regarding claim 1, Kaufman discloses each of the limitations of claim 17 that recite subject matter similar to that of claim 1. Further, Kaufman discloses the well-known use of computer memory to store information at least at page 215. Computer-readable instructions correspond to the software performing the functions disclosed in the reference. See Kaufman at pages 103, 104, 143, and 144. Accordingly, Kaufman fully anticipates the limitations of claim 17.

Claims 20, 26 and 28 - 31 depend directly or ultimately from claim 17 and include further

Petitioner Apple Inc. - Exhibit 1002, p. 452

limitations that are disclosed in Kaufman, as shown in Appendix D. The limitations recited in claims 20, 26 and 28 - 31 map closely to the limitations recited in claims 4, 10 and 12 - 15, respectively. Accordingly, for this reason, for the reasons discussed above regarding claim 17, for the reasons discussed above regarding claims 4, 10 and 12 - 15, and based upon the citations presented in Appendix D, it is respectfully asserted that each of the limitations of claims 20, 26 and 28 - 31 is fully disclosed in Kaufman, which therefore anticipates each of claims 20, 26 and 28 - 31.

As also discussed above in Section V(SNQ #1), independent claim 33 is directed to subject matter similar to that recited in claim 1, except that claim 33 is styled as a data processing apparatus comprising a processor and memory storing instructions for performing the steps recited in claim 1. As discussed above regarding claim 1, the Kaufman discloses each of the limitations of claim 33 that recite subject matter similar to that of claim 1. Further, Kaufman discloses the well-known data processing apparatus and processors in conjunction with the use of computers across networks, including the Internet. See Kaufman at pages 103, 104, 141, and 142. Accordingly, Kaufman fully anticipates the limitations of claim 33.

Claim 35 depends directly or ultimately from claim 33 and includes further limitations that are disclosed in the Kaufman, as shown in Appendix D. The limitations recited in claim 35 map closely to the limitations recited in claim 4. Accordingly, for this reason, for the reasons discussed above regarding claim 33, for the reasons discussed above regarding claim 4, and based upon the citations presented in Appendix D, it is respectfully asserted that each of the limitations of claim 35 is fully disclosed in Kaufman, which therefore anticipates claim 35.

For the reasons presented above, it is respectfully submitted that each of claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 of the '180 patent is fully disclosed, and therefore anticipated under 35 U.S.C. § 102(a), by the Kaufman prior art reference.

Petitioner Apple Inc. - Exhibit 1002, p. 453

SNQ #5 **Claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 are unpatentable under 35 U.S.C. § 103 for being obvious over Kaufman in view of Galvin**

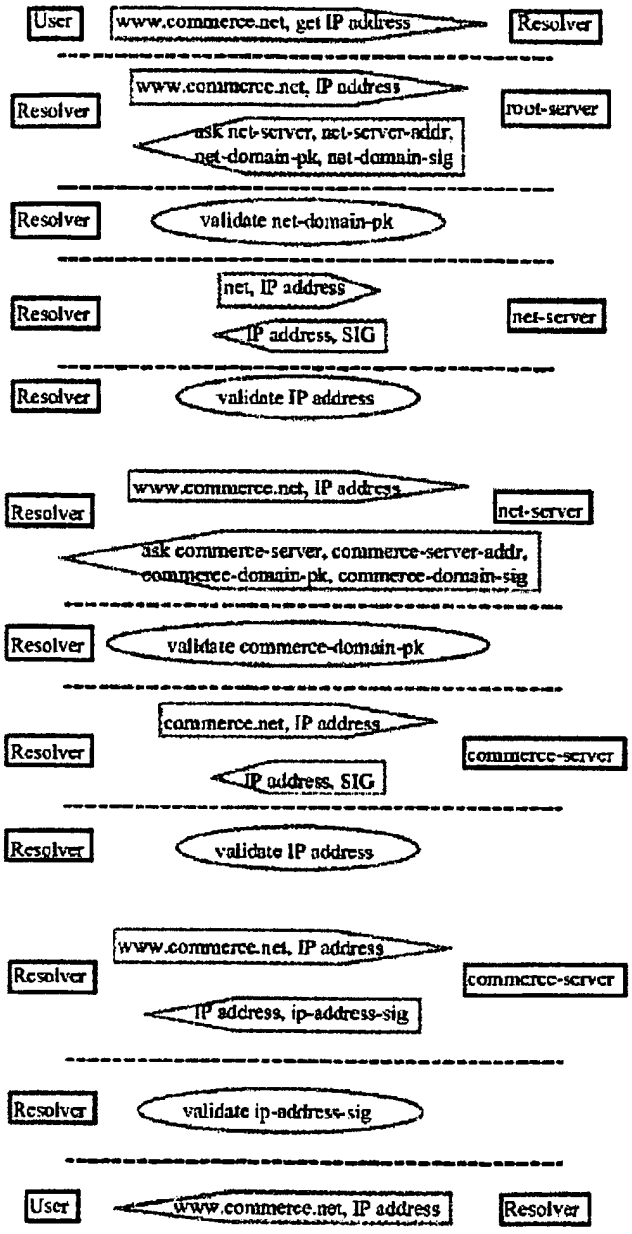
1. Substantial New Question of Patentability

Kaufman/Galvin's disclosure of requesting a secure computer network address from a secure domain name server according to the secure domain name and using a virtual private network communication link to send an access request message to the secure computer network address presents a new, non-cumulative technical teaching that was not previously considered and discussed on the record during prosecution of the '180 patent application (*i.e.*, the Kaufman and Galvin teachings are "new"). In particular, it is submitted that, based on the Examiner's statement of reasons for allowance, the claims of the '180 patent application were allowed because the references of record allegedly lacked requesting a secure computer network address from a secure domain name server according to the secure domain name, which is an element recited in independent claims 1, 17, and 33. As discussed below, the Kaufman/Galvin combination discloses each of these claimed elements and more.

2. Brief Description of the Prior Art

Kaufman is described above in Section V(SNQ #4). Galvin discusses a second type of secure domain name service that enhances the security of the Domain Name System by cryptographically binding domain names to their resources. Page 5. Specifically, Galvin discloses that the resource records managed by the DNS are digitally signed. Section 3.2 of Galvin provides an example of a DNS lookup where the DNS is secured with digitally signed records. A user issues a DNS lookup request to the local resolver, which sends the request along with a public key to the root server. The root server, in this case, does not have the necessary information for the DNS lookup; so it directs the local resolver to look to the net-domain for the lookup information. The local resolver can trust the response from the root server (i.e., the root server is secure) because the resolver and the root server share the appropriate public and private keys to the signed records. Eventually the resolver is directed to a DNS server that can answer the DNS lookup request. As before, the local resolver can trust that the DNS server is secure based on the successful validation of the public key.

Petitioner Apple Inc. - Exhibit 1002, p. 454



Petitioner Apple Inc. - Exhibit 1002, p. 455

3. Application of the Prior Art

As discussed above in Section V(SNQ #1), independent claim 1 is directed to a method for accessing a secure computer network address, comprising the steps of receiving a secure domain name; sending a query message to a secure domain name service for the corresponding network address; receiving a response message from the secure domain name service containing the network address; and sending an access request message to the secure computer network address using a VPN communication link.

Each of the steps of claim 1 is disclosed in the Kaufman reference as described above in Section V(SNQ #4). Each of the steps of claim 1 are also disclosed between the Kaufman and Galvin references, which are the subject of this SNQ. The Kaufman and Galvin references were published in 1999 and 1996, respectively, before the April 26, 2000 filing of the '209 CIP patent application. As discussed above, the disclosure of the '180 patent that provides written descriptive support, if any, of the claims of the '180 patent was introduced to the specification with the April 26, 2000 filing of the '209 parent CIP application. As such, the Kaufman and Galvin references are prior art to the '180 patent claims. A claim chart showing exemplary description of each of the limitations recited in claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 of the '180 patent as found in Kaufman and Galvin is attached hereto as Appendix E.

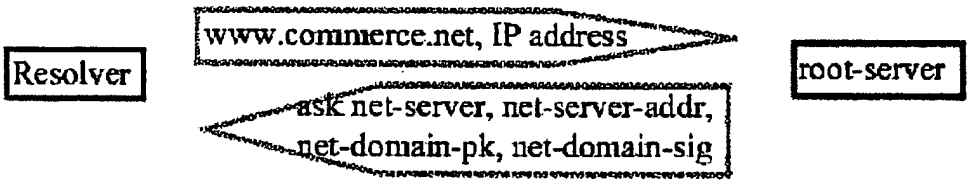
Kaufman's applicability to the claims is discussed in SNQ #4 and will not be repeated here. Galvin provides a second type of "secure domain name service" that includes digitally signed resource records. Secure domain name service is relevant for the following limitations in claim 1 (and the respective counterparts in claims 17 and 33):

> send a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name,
>
> receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name

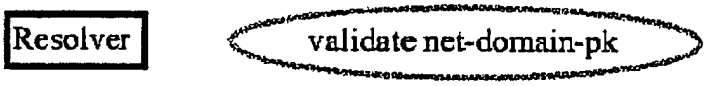
Galvin discloses these limitations at, for example, section 3.2, which discusses an example where a user issues a DNS lookup request for www.commerce.net. According to the example, the user issues a query message to the local resolver requesting the IP address corresponding to www.commerce.net.

Petitioner Apple Inc. - Exhibit 1002, p. 456

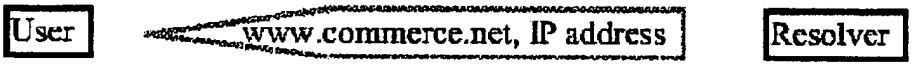
The local resolver is forwarded to several different DNS servers until a DNS server is reached that contains the corresponding IP address.



At each step, the local server validates the DNS server using the public key.



The appropriate DNS server returns the IP address corresponding to the domain name in the DNS lookup request.



Accordingly, when the type of secure DNS server disclosed in Galvin receives the DNS lookup request described in Kaufman, the secure DNS service will return the secure IP address corresponding to the request. This combination, therefore, meets the Court's construction in the Litigation that a "secure domain name service" means "a lookup service that returns a secure network address for a requested secure domain name." Exhibit 13 at page 32.

For the reasons presented above, it is respectfully submitted that each of claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 of the '180 patent is fully disclosed, and therefore rendered obvious under 35 U.S.C. § 103, by the Kaufman reference in view of the Galvin reference.

It would have been obvious to one of ordinary skill in the art to combine the Kaufman and Galvin references because one of ordinary skill in the art would have recognized that such a combination would have provided the predictable result of improving Kaufman. More particularly, Galvin discloses that its DNS "enhances or adds to the existing DNS, as opposed to

Petitioner Apple Inc. - Exhibit 1002, p. 457

changing or removing from the existing DNS." Galvin at page 8.

SNQ #6 **Claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 are unpatentable under 35 U.S.C. § 102(a) for being anticipated by Gauntlet**

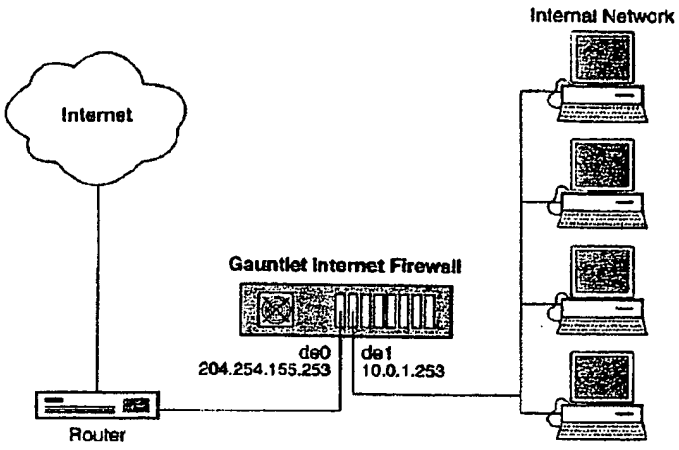
1. Substantial New Question of Patentability

Gauntlet's disclosure of requesting a secure computer network address from a secure domain name server according to the secure domain name and using a virtual private network communication link to send an access request message to the secure computer network address presents a new, non-cumulative technical teaching that was not previously considered and discussed on the record during prosecution of the '180 patent application (*i.e.*, the Gauntlet teaching is "new"). In particular, it is submitted that, based on the Examiner's statement of reasons for allowance, the claims of the '180 patent application were allowed because the references of record allegedly lacked requesting a secure computer network address from a secure domain name server according to the secure domain name, which is an element recited in independent claims 1, 17, and 33. As discussed below, Gauntlet discloses each of these claimed elements and more.

2. Brief Description of the Prior Art

Gauntlet is the administrator guide for the Gauntlet Firewall for Windows NT product and is another prior art reference discussing PPTP. In particular, Gauntlet discusses PPTP in the context of firewalls and security services. Gauntlet Firewall includes several security services for a number of popular applications - e.g. HTTP, PPTP, LDAP, FTP, and POP3. Each application generally talks through a different proxy service at the firewall. When traffic arrives at the firewall, the firewall evaluates whether the traffic is permitted. If it is, the traffic is passed to the appropriate proxy. PPTP, as previously mentioned, is one such proxy service offered by the Gauntlet Firewall and is described in detail beginning at page 18-1.

Petitioner Apple Inc. - Exhibit 1002, p. 458



3. Application of the Prior Art

As discussed above in Section V(SNQ #1), independent claim 1 is directed to a method for accessing a secure computer network address, comprising the steps of receiving a secure domain name; sending a query message to a secure domain name service for the corresponding network address; receiving a response message from the secure domain name service containing the network address; and sending an access request message to the secure computer network address using a VPN communication link.

Each of the steps of claim 1 is disclosed in the Gauntlet reference, which was published no later than 1999, before the April 26, 2000 filing of the '209 CIP patent application. As discussed above, the disclosure of the '180 patent that provides written descriptive support, if any, of the claims of the '180 patent was introduced to the specification with the April 26, 2000 filing of the '209 parent CIP application. As such, the 1999 Gauntlet is prior art to the '180 patent claims. A claim chart showing exemplary description of each of the limitations recited in claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 of the '180 patent as found in the Gauntlet reference is attached hereto as Appendix F.

The preamble of claim 1 requires "a method for accessing a secure computer network address." Gauntlet at page 18-1 discloses that PPTP connections can be established using the firewall. According to the Court in the Litigation, a "secure computer network address" means "a network address that requires authorization for access and is associated with a computer capable of virtual private network communications." Exhibit 13 at page 28. Gauntlet at pages 1-

Petitioner Apple Inc. - Exhibit 1002, p. 459

9 and 28-2 discloses that authentication may be required before access is granted to resources at the remote service.

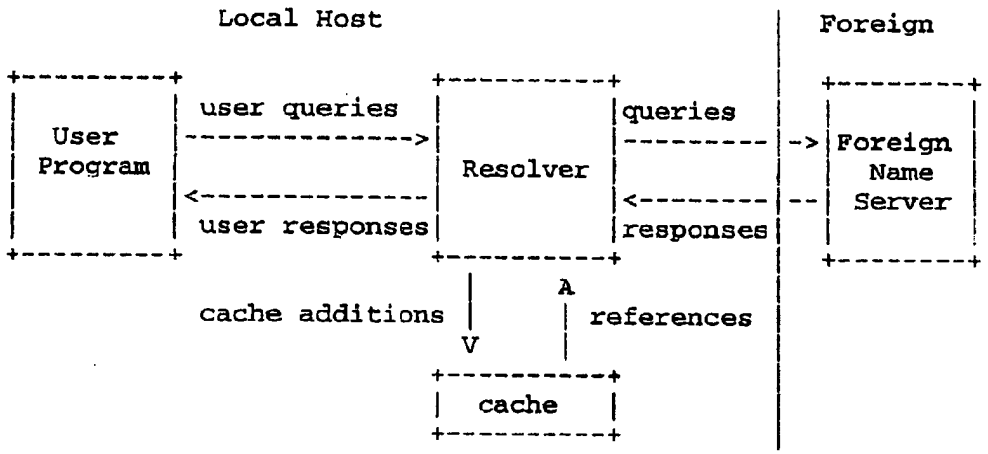
Claim 1 further requires, "receiving a secure domain name." According to the Court in the Litigation, a "secure domain name" means "a domain name that corresponds to a secure computer network address." Exhibit 13 at page 30. PPTP connections can be identified using domain names. See Gauntlet at pages 5-1, 5-2, 5-4, 20-1, and G-1, which illustrate that remote resources can be located using the domain name service. In the case where the domain name corresponds to a PPTP enabled server, the domain names is a secure domain name according to the Court's construction because the domain name corresponds to a secure network address (i.e., an address requiring authentication).

Claim 1 then requires "sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name." The Court in the Litigation construes "secure domain name service" broadly to include "a lookup service that returns a secure network address for a requested secure domain name." Exhibit 13 at page 32. Accordingly, a "secure domain name service" includes any lookup service that resolves a secure domain name.

Gauntlet discloses at pages 5-1, 5-2, 5-4, 20-1, and G-1 that the firewall includes a domain name services server to resolve domain names to corresponding network addresses. This DNS is a "secure" DNS according to the Court's construction because the DNS resolves a domain name for a PPTP enabled server.

The next limitation of claim 1 requires, "receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name." Gauntlet discloses such a feature at pages 5-1, 5-2, 5-4, 20-1, and G-1. As discussed in the previous paragraph, the firewall includes a DNS server to handle domain name resolution. DNS servers return the IP address corresponding to the received domain name. This is corroborated by RFC 1035 at page 4:

Petitioner Apple Inc. - Exhibit 1002, p. 460



The final limitation of claim 1 requires, "sending an access request message to the secure computer network address using a virtual private network communication link." Gauntlet discloses such a feature at page 18-1. The purpose of PPTP is to establish a VPN communication link so that the client computer can securely access resources using a public network. As introduced above, the subject matter recited in claim 1 of the '180 patent is fully disclosed in Gauntlet.

Claims 4, 10, and 12 - 15 depend directly or ultimately from claim 1 and include further limitations that are disclosed in Gauntlet, as shown in Appendix F. In brief illustration of select claims (Appendix F provides details for every claim):

For example, claim 4 recites that the response message contains provisioning information for the virtual private network. The Gauntlet reference, at least at pages 1-8 and 18-1 - 18-4, discloses the feature of providing resource information for allocating network resources, including hosts and ports.

Claim 10 recites the virtual private network includes the Internet, which is disclosed in the Gauntlet reference at least at pages 1-7 and 30-5.

Claim 12 recites that the access request message contains a request for information stored at the secure computer network address. This feature is disclosed in Gauntlet at least at page 18-1.

Claims 14 and 15 recite that the method of claim 1 is performed by a software module and that the method is performed by a client computer. The Gauntlet reference discloses a method for accessing a secure computer network address across a virtual private network. See

Petitioner Apple Inc. - Exhibit 1002, p. 461

Gauntlet at pages 1-4, 1-9, 18-1, and 30-5 and as in Appendix F. The Gauntlet reference discloses receiving a domain name at a software module (e.g., Internet browser, Windows NT, or other software that a user may use) on a client computer for a secure destination computer and sending the domain name to a Domain Name System server for mapping the domain name into a secure IP address. See Gauntlet at pages 1-8, 5-2, 18-1, and 30-5. The IP address is returned to the client computer, and a request is made to begin the secure connection to the specified destination computer. See Gauntlet at pages 1-7, 1-9, 5-1, 5-2, 5-4, 18-1, 20-1, and G-1.

Accordingly, for these reasons, for the reasons discussed above regarding claim 1, and based upon the citations presented in Appendix F, it is respectfully asserted that each of the limitations of claims 4, 10, and 12 - 15 is fully disclosed in the Gauntlet reference, which therefore anticipates each of claims 4, 10, and 12 - 15.

As also discussed above in Section V(SNQ #1), independent claim 17 is directed to subject matter similar to that recited in claim 1, except that claim 17 is styled as a computer-readable storage medium comprising a storage area and computer-readable instructions for performing the steps recited in claim 1. As discussed above regarding claim 1, the Gauntlet reference discloses each of the limitations of claim 17 that recite subject matter similar to that of claim 1. Further, the Gauntlet discloses the well-known use of computer memory to store information at least at pages 1-7, 10-1, and 18-1. While the Gauntlet reference does not expressly disclose computer-readable instructions, neither does the '180 patent; and such instructions are well-known parts of computer software application programs. See Gauntlet at pages 1-1 and 1-4. Accordingly, the Gauntlet reference fully anticipates the limitations of claim 17.

Claims 20, 26, and 28 - 31 depend directly or ultimately from claim 17 and include further limitations that are disclosed in the Gauntlet, as shown in Appendix F. The limitations recited in claims 20, 26, and 28 - 31 map closely to the limitations recited in claims 4, 10, and 12 - 15, respectively. Accordingly, for this reason, for the reasons discussed above regarding claim 17, for the reasons discussed above regarding claims 4, 10, and 12 - 15, and based upon the citations presented in Appendix F, it is respectfully asserted that each of the limitations of claims 20, 26, and 28 - 31 is fully disclosed in the Gauntlet reference, which therefore anticipates each of claims 20, 26, and 28 - 31.

As also discussed above in Section V(SNQ #1), independent claim 33 is directed to

Petitioner Apple Inc. - Exhibit 1002, p. 462

subject matter similar to that recited in claim 1, except that claim 33 is styled as a data processing apparatus comprising a processor and memory storing instructions for performing the steps recited in claim 1. As discussed above regarding claim 1, the Gauntlet discloses each of the limitations of claim 33 that recite subject matter similar to that of claim 1. Further, the Gauntlet reference discloses the well-known data processing apparatus and processors in conjunction with the use of computers across networks, including the Internet. See Gauntlet at pages 1-1, 1-7, and 18-1. Accordingly, the Gauntlet reference fully anticipates the limitations of claim 33.

Claim 35 depends from claim 33 and include further limitations that are disclosed in the Gauntlet reference, as shown in Appendix F. The limitations recited in claim 35 map closely to the limitations recited in claim 4. Accordingly, for this reason, for the reasons discussed above regarding claim 33, for the reasons discussed above regarding claim 4, and based upon the citations presented in Appendix F, it is respectfully asserted that each of the limitations of claim 35 is fully disclosed in the Gauntlet reference, which therefore anticipates claim 35.

For the reasons presented above, it is respectfully submitted that each of claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 of the '180 patent is fully disclosed, and therefore anticipated under 35 U.S.C. § 102(a), by the Gauntlet prior art reference.

SNQ #7 **Claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 are unpatentable under 35 USC § 103(a) for being obvious over Hands On in view of Installing NT**

1. Substantial New Question of Patentability

Hands On/Installing NT's disclosure of requesting a secure computer network address from a secure domain name server according to the secure domain name and using a virtual private network communication link to send an access request message to the secure computer network address presents a new, non-cumulative technical teaching that was not previously considered and discussed on the record during prosecution of the '180 patent application (*i.e.*, the Hands On and Installing NT teachings are "new"). In particular, it is submitted that, based on the Examiner's statement of reasons for allowance, the claims of the '180 patent application were allowed because the references of record allegedly lacked requesting a secure computer network address from a secure domain name server according to the secure domain name, which

Petitioner Apple Inc. - Exhibit 1002, p. 463

is an element recited in independent claims 1, 17, and 33. As discussed below, the Hands On/Installing NT combination discloses each of these claimed elements and more.

2. Brief Description of the Prior Art

Long before the applicant filed the application that became '180 patent, the Windows NT 4.0 software system included a virtual private networking protocol called PPTP. PPTP, as described in Hands On and Installing NT, is a network protocol that enables the secure transfer of data from a remote client to a private enterprise server, thus creating a virtual private network (VPN) over TCP/IP-based data networks, including local area networks (LANs), wide area networks (WANs), and the Internet and other public, TCP/IP-based networks.

PPTP requires the installation and configuration of the PPTP software at both the client computer and the PPTP server. Once configured, the user at the client computer creates a "phonebook" entry that contains the necessary details for the client computer to establish a PPTP connection with the PPTP server. The entry includes the PPTP server domain name, IP address, and other information.

In addition to the PPTP network protocol, the Windows NT 4.0 software system included an automatic dialing feature called AutoDial. AutoDial, as described in Hands On, is a feature that remembers the network connections made by users at the client computer and automatically configures these connections the next time the client computer makes the same connection request. AutoDial remembers these connections by mapping connection requests to their respective phonebook entries. In practice, a user requests a particular destination using the command line or alternatively, using an icon. See Hands On at page 462. AutoDial takes this input, recognizes the destination, and launches the appropriate phonebook entry.

Between these two features, Windows NT 4.0, as described by Hands On and Installing NT discloses a method for access a secure computer network according to the '180 patent.

3. Application of the Prior Art

As discussed above in Section V(SNQ #1), independent claim 1 is directed to a method for accessing a secure computer network address, comprising the steps of receiving a secure domain name; sending a query message to a secure domain name service for the corresponding network address; receiving a response message from the secure domain name service containing

Petitioner Apple Inc. - Exhibit 1002, p. 464

the network address; and sending an access request message to the secure computer network address using a VPN communication link.

Each of the steps of claim 1 is disclosed in the Hands On or Installing NT references, which were published in 1998 and 1997, respectively, before the April 26, 2000 filing of the '209 CIP patent application. As discussed above, the disclosure of the '180 patent that provides written descriptive support, if any, of the claims of the '180 patent was introduced to the specification with the April 26, 2000 filing of the '209 parent CIP application. As such, Hands On and Installing NT are prior art to the '180 patent claims. A claim chart showing exemplary description of each of the limitations recited in claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 of the '180 patent as found in Hands On and Installing NT is attached hereto as Appendix G.

The preamble of claim 1 requires "a method for accessing a secure computer network address." Hands On discloses such a feature at page 432. PPTP is a network protocol for accessing PPTP enabled network addresses. According to the Court in the Litigation, a "secure computer network address" means "a network address that requires authorization for access and is associated with a computer capable of virtual private network communications." Exhibit 13 at page 28. Hands On discloses at pages 435, 438, and 447 that Windows NT clients and servers may require authentication before access is granted to resources at the remote service.

Claim 1 further requires, "receiving a secure domain name." According to the Court in the Litigation, a "secure domain name" means "a domain name that corresponds to a secure computer network address." Exhibit 13 at page 30. PPTP connections can be identified using domain names. See figure below from page 21 of Installing NT, which illustrates that a PPTP server can be named "pptpserver.mycompany.com." This name corresponds to a secure network address – i.e., the address of the PPTP server. The client computer receives the domain name from the user in the form of a command line or icon.

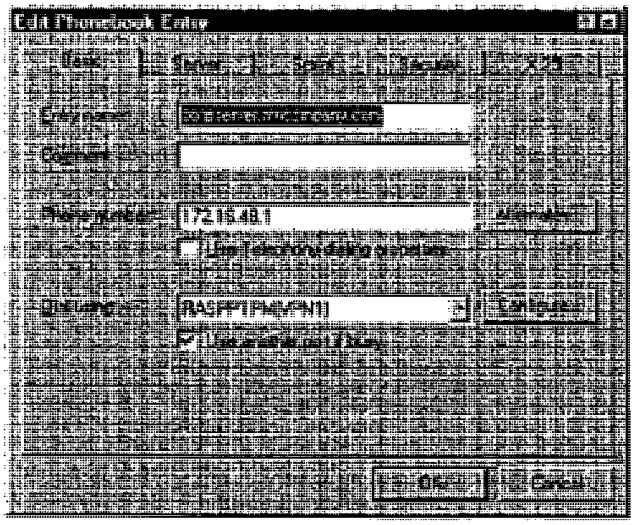


Figure 12 - Example Phonebook entry for PPTP server and a VPN device

Claim 1 then requires "sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name." The Court in the Litigation construes "secure domain name service" broadly to include "a lookup service that returns a secure network address for a requested secure domain name." Exhibit 13 at page 32. Accordingly, a "secure domain name service" includes any lookup service that resolves a secure domain name.

There are two "lookup services" described in Hands On that independently satisfy this limitation. The first "lookup service" is the traditional DNS server as defined by the Internet Engineering Task Force (IETF). Hands On discloses this feature at page 401 in an aptly named section called "How DNS Works." The first step is sending a query message to the DNS server requesting the corresponding IP address. Using the example in the figure above, when a user at the client computer tries to connect to "pptpserver.mycompany.com," the client computer sends a request to the secure DNS server (i.e., one capable of resolving the domain name) to resolve the secure domain name to the IP address.

The alternative "lookup service" disclosed in Hands On is AutoDial. If AutoDial is configured properly, it will return the phonebook entry corresponding to the domain name. Put another way, the client computer can request from AutoDial the IP address, which is part of the phonebook entry. See Hands On at page 462, describing how AutoDial maps domain names to

corresponding IP addresses.

The next limitation of claim 1 requires, "receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name." As discussed above, there are two "lookup services" disclosed in Hands On that independently satisfy the secure domain name service limitation. In both cases, the domain name is resolved to an IP address that is passed back to the client computer. With respect to the traditional DNS server, this is disclosed in Hands On at page 401. With respect to AutoDial, this is disclosed in Hands On at page 462, which describes how AutoDial maps domain names to their respective IP addresses. When AutoDial receives the domain name, it returns the appropriate phonebook entry with the IP address.

The final limitation of claim 1 requires, "sending an access request message to the secure computer network address using a virtual private network communication link." Hands On discloses such a feature at page 431. The purpose of PPTP is to establish a VPN communications link so that the client computer can securely access resources using a public network. As introduced above, the subject matter recited in claim 1 of the '180 patent is fully disclosed in Hands On and Installing NT.

Claims 4, 10, and 12-15 depend directly or ultimately from claim 1 and include further limitations that are disclosed in the Hands On or Installing NT, as shown in Appendix G. In brief illustration of select claims (Appendix G provides details for every claim):

Claim 4 recites that the response message contains provisioning information for the virtual private network. Installing NT discloses in its abstract that PPTP can be used to establish secure virtual networks using dial-up lines, local area networks, wide area networks, or the Internet. A PPTP-enabled client computer must have at least two phonebook entries describing its access server ports, i.e., resources, to the VPN. Pages 20 - 23. The address of the servers can be specified by their IP address or through a domain name service. Page 21. Once the initial network access is made, the network responds with network resource information from a phonebook entry, including network protocols and particular network adapters. Pages 20 - 23. In the figure on page 21, the network adapter is identified as RASPPTPM(VPN1). Further on at page 20, there is additional provisioning information including the connection protocol (TCP/IP) and whether compression is enabled.

Claim 10 recites the virtual private network includes the Internet, which is disclosed in

Petitioner Apple Inc. - Exhibit 1002, p. 467

Hands On at least at page 431.

Claim 12 recites that the access request message contains a request for information stored at the secure computer network address. This feature is disclosed in Hands On at least at page 431.

Claims 14 and 15 recite that the method is performed by a software module and that the method is performed by a client computer. More particularly, Windows NT 4.0, a software module, is installed at the client computer and configured for PPTP. Windows NT 4.0 receives a secure domain name from a user, sends the secure domain name for resolution, receives the corresponding secure network address, and subsequently sends an access request to the secure network address. See the discussion above regarding claim 1.

Accordingly, for these reasons, for the reasons discussed above regarding claim 1, and based upon the citations presented in Appendix G, it is respectfully asserted that each of the limitations of claims 1, 4, 10, and 12-15 is fully disclosed in the Hands On or Installing NT references, which therefore renders obvious each of claims 1, 4, 10, and 12-15.

As also discussed above in Section V(SNQ #1), independent claim 17 is directed to subject matter similar to that recited in claim 1, except that claim 17 is styled as a computer-readable storage medium comprising a storage area and computer-readable instructions for performing the steps recited in claim 1. As discussed above regarding claim 1, the Hands On reference in view of Installing NT disclose each of the limitations of claim 17 that recite subject matter similar to that of claim 1. Further, Hands On discloses the well-known use of computer memory to store information at least at page 428. While Hands On does not expressly disclose computer-readable instructions, neither does the '180 patent; and such instructions are well-known parts of computer software application programs. See Hands On at page 428. Accordingly, Hands On in view of Installing NT fully discloses the limitations of claim 17.

Claims 20, 26, and 28 - 31 depend directly or ultimately from claim 17 and include further limitations that are disclosed in Hands On, as shown in Appendix G. The limitations recited in claims 20, 26, and 28 - 31 map closely to the limitations recited in claims 4, 10, and 12 - 15, respectively. Accordingly, for this reason, for the reasons discussed above regarding claim 17, for the reasons discussed above regarding claims 4, 10, and 12 - 15, and based upon the citations presented in Appendix G, it is respectfully asserted that each of the limitations of claims 20, 26, and 28 - 31 is fully disclosed by Hands On in view of Installing NT, which therefore

Petitioner Apple Inc. - Exhibit 1002, p. 468

render obvious each of claims 20, 26, and 28 - 31.

As also discussed above in Section V(SNQ #1), independent claim 33 is directed to subject matter similar to that recited in claim 1, except that claim 33 is styled as a data processing apparatus comprising a processor and memory storing instructions for performing the steps recited in claim 1. As discussed above regarding claim 1, Hands On in view of Installing NT discloses each of the limitations of claim 33 that recite subject matter similar to that of claim 1. Further, Hands On discloses the well-known data processing apparatus and processors in conjunction with the use of computers across networks, including the Internet. See Hands On at page 428. Accordingly, Hands On in view of Installing NT fully anticipates the limitations of claim 33.

Claim 35 depends directly from claim 33 and includes a further limitation that is disclosed in Hands On, as shown in Appendix G. The limitation recited in claim 33 maps closely to the limitation recited in claim 4. Accordingly, for this reason, for the reasons discussed above regarding claim 33, for the reasons discussed above regarding claim 4, and based upon the citations presented in Appendix G, it is respectfully asserted that each of the limitations of claims 35 is fully disclosed in Hands On in view of Installing NT, which therefore renders claim 35 obvious.

There are several reasons to combine the Hands On and Installing NT references in the manner discussed above to render claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 obvious. See *KSR Int'l v. Teleflex, Inc.*, 127 S.Ct. 1727, 1733, 1743-44. First and foremost, both references concern the use of PPTP and Windows NT 4.0 for establishing VPNs. See Hands On at page 431 and Installing NT at abstract. One of ordinary skill in the art would have recognized that it would have been common sense to combine the references because they discuss the same product. Similarly, one of ordinary skill in the art would have recognized that the combination of the two references would have led to predictable results – again, because the references discuss the same product.

For the reasons presented above, it is respectfully submitted that each of claims 1, 4, 10, 12 - 15, 17, 20, 26, 28 - 31, 33, and 35 of the '180 patent is fully disclosed, and therefore rendered obvious under 35 U.S.C. § 103(a), by Hands On in view of Installing NT.

Petitioner Apple Inc. - Exhibit 1002, p. 469

SNQ #8 **Claims 1, 10, 12 - 15, 17, 26, 28 - 31, and 33 are unpatentable under 35 U.S.C. § 102(a) for being anticipated by Microsoft VPN**

1. Substantial New Question of Patentability

Microsoft VPN's disclosure of requesting a secure computer network address from a secure domain name server according to the secure domain name and using a virtual private network communication link to send an access request message to the secure computer network address presents a new, non-cumulative technical teaching that was not previously considered and discussed on the record during prosecution of the '180 patent application (*i.e.*, the Microsoft VPN teaching is "new"). In particular, it is submitted that, based on the Examiner's statement of reasons for allowance, the claims of the '180 patent application were allowed because the references of record allegedly lacked requesting a secure computer network address from a secure domain name server according to the secure domain name, which is an element recited in independent claims 1, 17, and 33. As discussed below, Microsoft VPN discloses each of these claimed elements and more.

2. Brief Description of the Prior Art

The Microsoft VPN reference is another prior art reference regarding PPTP and discusses Virtual Private Networking technology in the context of Windows NT 4.0. In particular, Microsoft VPN discusses the use of VPNs for corporate users that are working remotely. The reference provides significant detail concerning the PPTP data packets, network routing concerns, and security. Figure 1 illustrates the logical concept of a VPN.

Petitioner Apple Inc. - Exhibit 1002, p. 470

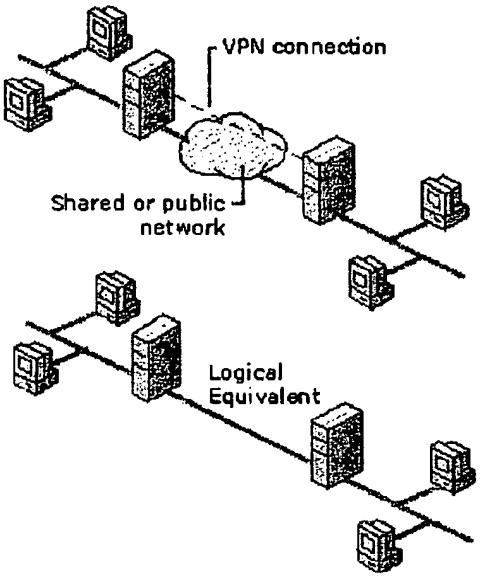


Figure 1 Virtual Private Network (VPN)

3. Application of the Prior Art

As discussed above in Section V(SNQ #1), independent claim 1 is directed to a method for accessing a secure computer network address, comprising the steps of receiving a secure domain name; sending a query message to a secure domain name service for the corresponding network address; receiving a response message from the secure domain name service containing the network address; and sending an access request message to the secure computer network address using a VPN communication link.

Each of the steps of claim 1 is disclosed in the Microsoft VPN reference, which was published January 1, 2000, before the April 26, 2000 filing of the '209 CIP patent application. As discussed above, the disclosure of the '180 patent that provides written descriptive support, if any, of the claims of the '180 patent was introduced to the specification with the April 26, 2000 filing of the '209 parent CIP application. As such, the Microsoft VPN is prior art to the '180 patent claims. A claim chart showing exemplary description of each of the limitations recited in claims 1, 10, 12 - 15, 17, 26, 28 - 31, and 33 of the '180 patent as found in the Microsoft VPN reference is attached hereto as Appendix H.

The preamble of claim 1 requires "a method for accessing a secure computer network

Petitioner Apple Inc. - Exhibit 1002, p. 471

address." Microsoft VPN at page 11 discloses that PPTP connections can be established to secure communication paths across a public network. According to the Court in the Litigation, a "secure computer network address" means "a network address that requires authorization for access and is associated with a computer capable of virtual private network communications." Exhibit 13 at page 28. Microsoft VPN discloses that authentication may be required before access is granted to resources at the remote service. See page 13.

Claim 1 further requires, "receiving a secure domain name." According to the Court in the Litigation, a "secure domain name" means "a domain name that corresponds to a secure computer network address." Exhibit 13 at page 30. PPTP connections can be identified using domain names. See Microsoft VPN at page 32, which discloses that the VPN server can be addresses using either the host name or the IP address. In the case where the domain name corresponds to a PPTP enabled server, the domain names is a secure domain name according to the Court's construction because the domain name corresponds to a secure network address (i.e., an address requiring authentication).

Claim 1 then requires "sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name." The Court in the Litigation construes "secure domain name service" broadly to include "a lookup service that returns a secure network address for a requested secure domain name." Exhibit 13 at page 32. Accordingly, a "secure domain name service" includes any lookup service that resolves a secure domain name.

Microsoft VPN discloses that domain names are sent to a domain name services server for resolution. In other words, a query message is sent to the domain name services server for the IP address corresponding to the domain name. See pages 63 - 66. This DNS is a "secure" DNS according to the Court's construction because the DNS resolves a domain name for a PPTP enabled server.

The next limitation of claim 1 requires, "receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name." Microsoft VPN discloses such a feature at pages 63 - 66. DNS servers return the IP address corresponding to the received domain name.

The final limitation of claim 1 requires, "sending an access request message to the secure computer network address using a virtual private network communication link." MS VPN

Petitioner Apple Inc. - Exhibit 1002, p. 472

discloses such a feature at pages 11 - 12. The purpose of PPTP is to establish a VPN communication link so that the client computer can securely access resources using a public network. See Microsoft VPN at page 11. As introduced above, the subject matter recited in claim 1 of the '180 patent is fully disclosed in Microsoft VPN.

Claims 10 and 12 - 15 depend directly or ultimately from claim 1 and include further limitations that are disclosed in the Microsoft VPN, as shown in Appendix H. In brief illustration of select claims (Appendix H provides details for every claim):

Claim 10 recites the virtual private network includes the Internet, which is disclosed in the Microsoft VPN reference at least at page 34.

Claim 12 recites that the access request message contains a request for information stored at the secure computer network address. This feature is disclosed in Microsoft VPN at least at page 11.

Claims 14 and 15 recite that the method of claim 1 is performed by a software module and that the method is performed by a client computer. The Microsoft VPN reference discloses a method for accessing a secure computer network address across a virtual private network. See Microsoft VPN at pages 11, 13, and 34 and as in Appendix H. The Microsoft VPN reference discloses receiving a domain name at a software module (i.e., Windows NT 4.0) on a client computer for a secure destination computer and sending the domain name to a Domain Name System server for mapping the domain name into a secure IP address. See Microsoft VPN at pages 11, 13, 32, and 35. The IP address is returned to the software module on the client computer, and a request is made to begin the secure connection to the specified destination computer. See Microsoft VPN at pages 11, 13, and 16. As introduced above, the subject matter recited in claims 14 and 15 of the '180 patent is fully disclosed in the Microsoft VPN.

Accordingly, for these reasons, for the reasons discussed above regarding claim 1, and based upon the citations presented in Appendix H, it is respectfully asserted that each of the limitations of claims 10 and 12 - 15 is fully disclosed by the Microsoft VPN reference, which therefore anticipates each of claims 10 and 12 - 15.

As also discussed above in Section V(SNQ #1), independent claim 17 is directed to subject matter similar to that recited in claim 1, except that claim 17 is styled as a computer-readable storage medium comprising a storage area and computer-readable instructions for performing the steps recited in claim 1. As discussed above regarding claim 1, the Microsoft

Petitioner Apple Inc. - Exhibit 1002, p. 473

VPN reference discloses each of the limitations of claim 17 that recite subject matter similar to that of claim 1. Further, the Microsoft VPN discloses the well-known use of computer memory to store information at least at pages 11, 15, and 16. Computer-readable instructions correspond to the software performing the functions disclosed in the reference. See Microsoft VPN at pages 11 and 37. Accordingly, the Microsoft VPN reference anticipates each of the limitations of claim 17.

Claims 26 and 28 - 31 depend directly or ultimately from claim 17 and include further limitations that are disclosed in the Microsoft VPN, as shown in Appendix H. The limitations recited in claims 26 and 28 - 31 map closely to the limitations recited in claims 10 and 12 - 15, respectively. Accordingly, for this reason, for the reasons discussed above regarding claim 17, for the reasons discussed above regarding claims 10 and 12 - 15, and based upon the citations presented in Appendix H, it is respectfully asserted that each of the limitations of claims 26 and 28 - 31 is fully disclosed in the Microsoft VPN reference, which therefore anticipates each of claims 26 and 28 - 31.

As also discussed above in Section V(SNQ #1), independent claim 33 is directed to subject matter similar to that recited in claim 1, except that claim 33 is styled as a data processing apparatus comprising a processor and memory storing instructions for performing the steps recited in claim 1. As discussed above regarding claim 1, the Microsoft VPN discloses each of the limitations of claim 33 that recite subject matter similar to that of claim 1. Further, the Microsoft VPN reference discloses the well-known data processing apparatus and processors in conjunction with the use of computers across networks, including the Internet. See Microsoft VPN at pages 11, 27, 28, 34, and 37. Accordingly, the Microsoft VPN reference anticipates the limitations of claim 33.

For the reasons presented above, it is respectfully submitted that each of claims 1, 10, 12 - 15, 17, 26, 28 - 31, and 33 of the '180 patent is fully disclosed, and therefore anticipated under 35 U.S.C. § 102(a), by the Microsoft VPN prior art reference.

Petitioner Apple Inc. - Exhibit 1002, p. 474

Summary

The new, non-cumulative prior art documents referred to above were not considered by the Examiner during prosecution of the '180 patent application. Since each of the limitations of claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of the '180 patent is disclosed in these documents, contrary to the statement of reasons for allowance, a substantial new question of patentability is raised. Accordingly, the Requestor respectfully asks that this Request for *Inter Partes* Reexamination be granted and that the claims of the '180 patent be reexamined in view of the prior art presented herein.

If any fees are required in connection with this Request, please charge the same to our Deposit Account No. 02-2135.

Respectfully submitted,

ROTHWELL, FIGG, ERNST & MANBECK, P.C.

By: _____

William N. Hughet
Reg. No. 44,481

Rothwell, Figg, Ernst & Manbeck, P.C.
1425 K Street, NW
Suite 800
Washington, D.C. 20005
Telephone: (202) 626-3534
Facsimile: (202) 783-6031

Date: December 8, 2009

Petitioner Apple Inc. - Exhibit 1002, p. 475

CERTIFICATE OF SERVICE

I hereby certify that true and correct copies of the **Replacement Request for Inter Partes Reexamination of Patent**, were served via Federal Express, by the undersigned, on **December 8, 2009**, to:

VirnetX, Inc.
c/o Banner & Witcoff, Ltd.
1100 13th Street, N.W., Suite 1200
Washington, D.C. 20005-4051

&

VirnetX, Inc.
5615 Scotts Valley Drive, Suite 110
Scotts Valley, CA 95066

A copy of the Federal Express Receipts are attached hereto.

Tamika Miles

From: Origin ID: JPNA (202) 626-3565
Tamika Miles
Rothwell, Figg, Ernst
1425 K Street, N.W.
Suite 800
Washington, DC 20005

FedEx Express

Ship Date: 08DEC09
ActWgt: 1.0 LB
CAD: 1139317/INET9090
Account#: S *********

Delivery Address Bar Code

SHIP TO: (831) 438-8200 BILL SENDER

VirnetX, Inc.
5615 SCOTTS VALLEY DR STE 110

SCOTTS VALLEY, CA 95066

Ref # 3755-180
Invoice #
PO #
Dept #

TRK# 0201 7982 0381 2579

WED - 09DEC A5
PRIORITY OVERNIGHT

XX SRUA

95066
CA-US
SJC

After printing this label:
1. Use the 'Print' button on this page to print your label to your laser or inkjet printer.
2. Fold the printed page along the horizontal line.
3. Place label in shipping pouch and affix it to your shipment so that the barcode portion of the label can be read and scanned.

Warning: Use only the printed original label for shipping. Using a photocopy of this label for shipping purposes is fraudulent and could result in additional billing charges, along with the cancellation of your FedEx account number.

Use of this system constitutes your agreement to the service conditions in the current FedEx Service Guide, available on fedex.com.FedEx will not be responsible for any claim in excess of $100 per package, whether the result of loss, damage, delay, non-delivery,misdelivery,or misinformation, unless you declare a higher value, pay an additional charge, document your actual loss and file a timely claim.Limitations found in the current FedEx Service Guide apply. Your right to recover from FedEx for any loss, including intrinsic valueof the package, loss of sales, income interest, profit, attorney's fees, costs, and other forms of damage whether direct, incidental,consequential, or special is limited to the greater of $100 or the authorized declared value. Recovery cannot exceed actual documented loss.Maximum for items of extraordinary value is $500, e.g. jewelry, precious metals, negotiable instruments and other items listed in our ServiceGuide. Written claims must be filed within strict time limits, see current FedEx Service Guide.

Electronic Acknowledgement Receipt

EFS ID:	6596968
Application Number:	95001270
International Application Number:	
Confirmation Number:	2128
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	7188180
Customer Number:	22907
Filer:	William Neal Hughet/Tamika Miles
Filer Authorized By:	William Neal Hughet
Attorney Docket Number:	3755-121
Receipt Date:	08-DEC-2009
Filing Date:	
Time Stamp:	17:50:09
Application Type:	Inter partes reexam

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Receipt of Corrected Original Inter Partes Request	ReplacementRequestforInterPartesReexam180.pdf	3576452 8547e3ae3cba1350b2738a3475382d3721621db6	no	57

Warnings:

Information:

2	Reexam Certificate of Service	CertificateofServicefor180.pdf	83560 fa499589dd2a3cc0e3c5b9d48bcf0541363f1766	no	2

Warnings:	
Information:	
Total Files Size (in bytes):	3660012

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Application Number	Application/Control No.	Applicant(s)/Patent Under Reexamination
	95/001,270	7188180
	Examiner	Art Unit
	.	3999

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	95001270	7188180
	Examiner	Art Unit
		3999

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	+	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original									
	41									

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	95001270	7188180
	Examiner	Art Unit
	.	3999

ORIGINAL		INTERNATIONAL CLASSIFICATION	
CLASS	SUBCLASS	CLAIMED	NON-CLAIMED
709	227		

CROSS REFERENCE(S)					
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original

(Assistant Examiner) (Date)	Total Claims Allowed:	
(Primary Examiner) (Date)	O.G. Print Claim(s)	O.G. Print Figure

Petitioner Apple Inc. - Exhibit 1002, p. 482

Reexamination	Application/Control No. 95001270	Applicant(s)/Patent Under Reexamination 7188180
	Certificate Date	Certificate Number

Requester Correspondence Address: ☐ Patent Owner ☒ Third Party
ROTHWELL, FIGG, RENST & MANBECK, P.C. 1425 K STREET N.W. SUITE 800 WASHINGTON, D.C. 20005

LITIGATION REVIEW ☐	(examiner initials)	(date)
Case Name		Director Initials

COPENDING OFFICE PROCEEDINGS	
TYPE OF PROCEEDING	NUMBER

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	95001270	7188180
	Examiner	Art Unit
		3999

SEARCHED			
Class	Subclass	Date	Examiner
709	227		

SEARCH NOTES		
Search Notes	Date	Examiner

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Bib Data Sheet

CONFIRMATION NO. 2128

SERIAL NUMBER	FILING OR 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
95/001,270	12/08/2009 RULE	709	3992	3755-121

APPLICANTS

7188180, Residence Not Provided;
VIRNETX INC.(OWNER), SCOTTSVALLEY DRIVE, CA;
MICROSOFT CORPORATION(3RD. PTY. REQ.), CHEVY CHASE, MD;
MICROSOFT CORPORATION(REAL PTY. IN INTEREST), CHEVY CHASE, MD;
ROTHWELL, FIGG, ERNST & MANBECK, P.C., WASHINGTON, DC

**** CONTINUING DATA ***************************

This application is a REX of 10/702,486 11/07/2003 PAT 7,188,180
which is a DIV of 09/558,209 04/26/2000 ABN
which is a CIP of 09/504,783 02/15/2000 PAT 6,502,135
which is a CIP of 09/429,643 10/29/1999 PAT 7,010,604
which claims benefit of 60/106,261 10/30/1998
and claims benefit of 60/137,704 06/07/1999

**** FOREIGN APPLICATIONS *********************

Foreign Priority claimed	STATE OR COUNTRY	SHEETS DRAWING	TOTAL CLAIMS	INDEPENDENT CLAIMS
☐ yes ☐ no				
35 USC 119 (a-d) conditions met ☐ yes ☐ no ☐ Met after Allowance				
Verified and Acknowledged Examiner's Signature Initials				

ADDRESS
22907

TITLE
METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

FILING FEE RECEIVED	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:

☐ All Fees
☐ 1.16 Fees (Filing)
☐ 1.17 Fees (Processing Ext. of time)
☐ 1.18 Fees (Issue)
☐ Other _____
☐ Credit

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

Requester's Name and Address: WILLIAM N. HUGHET
ROTHWELL, FIGG, ERNST & MANBECK, P.C.
1425 K STREET, NW, SUITE 800
WASHINGTON, DC 20005

Patent Number: 7,188,180 Request Receipt Date: 11-25-2009

Control Number: 95/001,270
Date Mailed: 12-03-2009

NOTICE OF FAILURE TO COMPLY WITH *INTER PARTES* REEXAMINATION REQUEST FILING REQUIREMENTS (37 CFR 1.915(d))

The Central Reexamination Unit (CRU) in the United States Patent and Trademark Office (USPTO) has received a request for *inter partes* reexamination. The request cannot be processed, because the below-identified filing date requirements for an *inter partes* reexamination request have not been satisfied. If a fully compliant response is not received within 30 days of the mailing date of this notice, the request will be treated as a prior art citation under 37 CFR 1.501 or closed from public view, at the Office's option. A filing date will NOT be assigned to the request until the deficiencies noted below are corrected (37 CFR 1.919(a)):

The following items required by 37 CFR 1.915 are missing:

☐ 1. The *inter partes* reexamination filing fee under 37 CFR 1.20(c)(2) – see Attached Form PTO-2057.

☐ 2. An identification of the patent by its patent number, and of every claim of the patent for which reexamination is requested.

☐ 3. A citation of the patents and printed publications that are presented to raise a substantial new question of patentability.

☒ 4. A statement pointing out each substantial new question of patentability based on the cited patents & printed publications, and a detailed explanation of the pertinency and manner of applying the patents & printed publications to every claim for which reexamination is requested.

☐ 5. A legible copy of every patent or printed publication (other than U.S. patents or U.S. patent publications) relied upon or referred to in (3) and (4) above, accompanied by an English language translation of all the necessary and pertinent parts of any non-English language document.

☐ 6. A legible copy of the entire patent including the front face, drawings, and specification/claims (in double column format) for which reexamination is requested, and a copy of any disclaimer, certificate of correction, or reexamination certificate issued in the patent. All copies must have each page plainly written on only one side of a sheet of paper.

☐ 7. A certification by the third party requester that a copy of the request has been served in its entirety on the patent owner at the address provided for in 37 CFR 1.33(c). The name and address of the party served must be indicated. If service was not possible, a duplicate copy of the request must be supplied to the Office.

☐ 8. A certification by the third party requester that the estoppel provisions of 37 CFR 1.907 do not prohibit the *inter partes* reexamination.

☐ 9. A statement identifying the real party in interest to the extent necessary for a subsequent person filing an *inter partes* reexamination request to determine whether that person is a privy of the real party in interest.

☒ 10. Other item: See Attachment.

☒ Explanation of above item(s): See Attachment.

Any written correspondence in response to this notice must include a submission pursuant to the attached instructions. **The instructions for a detailed explanation for an *inter partes* reexamination request differ from those for an *ex parte* reexamination request.** Any written correspondence in response to this notice should be mailed to the Central Reexamination Unit (CRU), ATTN: "Box *Inter Partes* Reexam" at the USPTO address indicated at the top of this notice. Any "replacement documents" may be facsimile transmitted to the CRU at the FAX number indicated below. A REPLACEMENT STATEMENT AND EXPLANATION UNDER 37 CFR 1.915(b)(3) MAY NOT BE FACSIMILE TRANSMITTED.

Manuel Salima

Patent Reexamination Specialist, Central Reexamination Unit
(571) 272-6825 ; FAX No. (571) 273-9900

cc: Patent Owner's Name and Address: BANNER & WITCOFF, LTD
1100 13TH STREET, NW
SUITE 1200
WASHINGTON, DC 20005-4051

ATTACHMENT TO PTOL-2076

Control Number: 95/001,270
Patent Number: 7,188,180
Request Receipt Date: 11/25/2009

A request for *inter partes* reexamination (or for *ex parte* reexamination) must now meet all the applicable statutory and regulatory requirements before a filing date is accorded to the request. See MPEP 2227 Part B.1 and MPEP 2217, Part I. See also *Clarification of Filing Date Requirements for Ex Parte and Inter Partes Reexamination Proceedings*, 71 Fed. Reg. 44219 (August 4, 2006), 1309 *Off. Gaz. Pat. Office* 216 (August 29, 2006) (final rule.)

The request submitted on November 25, 2009, cannot be processed because all of the filing date requirements for an *inter partes* reexamination have not been satisfied. The Request for Reexamination does not comply with the filing requirement of an *Inter Partes* reexamination proceeding under 37 CFR 1.915(b)(3), which requires "[a] statement pointing out each substantial new question of patentability based on the cited patents and printed publications, and a detailed explanation of the pertinency and manner of applying the patents and printed publications to every claim for which reexamination is requested.

Reexamination was requested for U.S. Patent No. 7,188,180 (in this instance claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33 and 35 are requested).

The request is incomplete as to compliance with 37 CFR 1.915(b)(3) for the following reason.

The request has failed to provide the requisite identification and explanation, in compliance with 37 CFR 1.915(b)(3), of what substantial new questions of patentability (SNQs) are being raised **by the cited prior art documents under 37 CFR 1.915(b)**. The request fails to clearly point out and explain how each asserted SNQ is substantially different from those raised in the previous examination of the patent before the Office. **It is not sufficient to merely state that the references were not of record in the prior prosecution of the '180 patent.** Also, as pointed out in MPEP 2616, "[i]t is not sufficient that a request for reexamination merely proposes one or more rejections of a patent claim or claims as a basis for reexamination. It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents **a new, non-cumulative technological teaching** that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during prosecution of any other prior proceeding involving the patent for which reexamination is requested." [Emphasis added]

Under 35 U.S.C. 311, the requester must "set forth the pertinency and manner of applying cited prior art to every claim for which reexamination is requested." Then, under 35 U.S.C. 312 and 313, the Office must determine whether "a substantial new question of patentability" affecting any claim of the patent has been raised by a request for reexamination.

To implement these statutory provisions, 37 CFR 1.915(b)(3) requires that the request include "a statement pointing out each substantial new question of patentability based on the cited patents and printed publications..." See MPEP 2617.

Accordingly, it is mandatory that the request clearly set forth in detail the specifics of what the third party requester considers the "substantial new question of patentability" to be. A request will point out how any questions of patentability raised are substantially different from those raised in the previous examination of the patent before the Office. See MPEP 2616.

If the requester were permitted to omit an explanation of how such documents cited in request are applied to the patent claims, an undue burden would be placed on the Office to address each document in the determination on the request, without an explanation of the relevance to the patent claims. Accordingly, such an omission is prohibited by law.

In view of the above discussion, the request does not provide a "statement pointing out each substantial new question of patentability based on the cited patents and printed publications, and a detailed explanation of the pertinency and manner of applying the patents and printed publications to every claim for which reexamination is requested," as is required by 37 CFR 1.915(b)(3).

In accordance with 37 CFR 1.915(b), a filing date for the reexamination request will not be granted **at this time.**

Requester has the option to respond to this identification of a defect by using the appropriate option(s) set forth below:

1. A replacement statement and explanation pursuant to 37 CFR 1.915(b)(3), as detailed in the attached instructions. A statement identifying a substantial new question of patentability and an accompanying explanation must be provided for **EACH** of the documents that the requester desires the Office to consider.

2. Requester may either submit an explanation of the pertinency and manner of applying each of the cited prior art documents for every claim for which reexamination is requested in accordance with 37 CFR 1.915(b)(3).

3. A replacement Form PTO/SB/08a PTO-1449, or equivalent listing ONLY those references (with proper page designation, where appropriate) discussed in a proposed rejection (or statement identifying a substantial new question) and in a corresponding explanation under 37 CFR 1.915(b)(3).

Failure to submit a proper response to this Notice may result in the termination of the request, with no filing date accorded.

All correspondence relating to this *inter partes* reexamination proceeding should be directed:

By EFS: Registered users may submit via the electronic filing system EFS-Web, at https://sportal.uspto.gov/authenticate/authenticateuserlocalepf.html.

By Mail to: Mail Stop *Inter Partes* Reexam
Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

By hand: Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

INSTRUCTIONS TO NOTICE OF FAILURE TO COMPLY WITH *INTER PARTES* REEXAMINATION REQUEST FILING REQUIREMENTS (37 CFR 1.915)

HOW TO REPLY TO THIS NOTICE

Any written correspondence in response to this notice must include either a **replacement document**, or, **if item #4 is checked and/or it is otherwise specifically required by the Office, a paper containing a replacement statement and explanation under 37 CFR 1.915(b)(3)** that either replaces the originally-filed statement and explanation or provides a previously missing statement and explanation. A replacement document either replaces an originally-filed document, or provides a previously missing document, that contains part(s) of the request other than the statement and explanation as set forth in 37 CFR 1.915(b)(3). For example, a replacement to the originally-filed listing of cited patents and printed publications, PTO/SB/08 (formerly designated as PTO-1449) or its equivalent, is a replacement document.

If a paper containing a replacement statement and explanation, or a replacement document (other than a replacement certificate of service), is submitted by a third party requester, it must be accompanied by a certification that a copy of the replacement statement and explanation under 37 CFR 1.915(b)(3), or that a copy of the replacement document, has been served in its entirety on the patent owner at the address provided for in 37 CFR 1.33(c). The name and address of the party served must be indicated. If service was not possible, a duplicate copy of the replacement statement and explanation (or replacement document) must be supplied to the Office.

REPLACEMENT STATEMENT AND EXPLANATION UNDER 37 CFR 1.915(b)(3) (ITEM #4 IS CHECKED)

The **statement and explanation under 37 CFR 1.915(b)(3)** (see item #4) must discuss **EVERY patent or printed publication cited in the information disclosure statement** in at least one proposed rejection or statement identifying a substantial new question of patentability (SNQ), AND in a corresponding detailed explanation (see the below discussion). Furthermore, **EVERY claim for which reexamination is requested** must be discussed in at least one proposed rejection or statement identifying an SNQ and in the corresponding detailed explanation. If item #4 is missing or incomplete, a paper containing a **replacement statement and explanation under 37 CFR 1.915(b)(3) is required.**

A paper containing a replacement statement and explanation under 37 CFR 1.915(b)(3) may NOT be facsimile transmitted. It must be received by first class mail or by U.S. Postal Service (USPS) Express Mail.

If an originally-filed information disclosure statement cites patents or printed publications that are NOT discussed in at least one proposed rejection or statement identifying an SNQ AND in the corresponding detailed explanation **in the originally-filed request**, then the requester must file either (a) a **replacement document, i.e., a replacement PTO/SB/08 (former PTO-1449)** or its equivalent, listing **ONLY** those patents and printed publications that are so discussed, or (b) a paper containing a **replacement statement and explanation under 37 CFR 1.915(b)(3).** If the first option is chosen, the replacement PTO/SB/08 or its equivalent should include a cover letter expressly withdrawing from the request any previously cited references that are being omitted by the replacement PTO/SB/08 or its equivalent. The requester may, if desired, file both a replacement PTO/SB/08 or its equivalent and a paper containing a replacement statement and explanation, if the replacement statement and explanation discusses EVERY patent or printed publication, cited in the replacement PTO/SB/08 or its equivalent, in at least one proposed rejection or statement identifying an SNQ and in the corresponding detailed explanation.

Requester is NOT required to, and should not, additionally file a replacement copy of any exhibits, references, etc., or other replacement parts of the request (i.e., replacement documents) if a defect requiring a replacement document is not specifically identified by this notice.

Examples of When a Replacement Statement and Explanation under 37 CFR 1.915(b)(3) Is Required:

1. The originally-filed request fails to discuss **EVERY** patent or printed publication cited in the originally-filed information disclosure statement in at least one proposed rejection or statement identifying an SNQ and in the corresponding detailed explanation, and the requester does not wish to file a replacement PTO/SB/08 (formerly designated as PTO-1449) or its equivalent listing ONLY those patents and printed publications that are so discussed.

2. The originally-filed request discusses every patent or printed publication cited in the information disclosure statement in at least one proposed rejection or statement identifying an SNQ, but **fails to discuss EVERY patent or printed publication cited in the information disclosure statement in a detailed explanation that corresponds to the proposed rejection or statement identifying an SNQ.**

3. The originally-filed request fails to discuss **EVERY CLAIM** for which reexamination is requested in at least one proposed rejection or statement identifying an SNQ, and in the corresponding detailed explanation.

Examples of Proposed Rejections and Statements Identifying a Substantial New Question of Patentability (SNQ)

Proposed rejections

Claims 1-3 are obvious over reference A in view of reference B.
Claims 4-6 are obvious over reference A in view of references B and C.
Claims 7-10 are obvious over reference Q in view of reference R.

Statements identifying a substantial new question of patentability

A substantial new question of patentability as to claims 1-3 is raised by reference A in view of reference B.
A substantial new question of patentability as to claims 4-6 is raised by reference A in view of references B and C.
A substantial new question of patentability as to claims 7-10 is raised by reference Q in view of reference R.

A proposed rejection or statement identifying an SNQ must be repeated with any *replacement* detailed explanation that corresponds to the proposed rejection or statement identifying an SNQ, in any paper containing a replacement statement and explanation under 37 CFR 1.915(b)(3).

In addition, the requester should include an explanation of *how the SNQ is raised.*

1. Assume that claim 1 of the patent recites, as one of the limitations, widget W. Requester would state that the XYZ reference, cited in the information disclosure statement, contains a teaching of widget W as recited in claim 1, and that this teaching was not present during the prior examination of the patent under reexamination (i.e., the teaching is "new"). Requester would also state that he believes that a reasonable examiner would consider this teaching important in determining whether or not the claims are patentable. For this reason, requester would state that this teaching by the XYZ reference raises a substantial new question of patentability (SNQ) with respect to at least claim 1 of the patent. Similarly, if dependent claim 6 adds widget H, the requester would state that the ABC reference, cited in the information disclosure statement, contains a teaching of widget H as recited in claim 6, that this teaching was not present during the prior examination of the patent, that a reasonable examiner would consider this teaching important in determining whether or not the claims are patentable, and that this teaching raises an SNQ with respect to dependent claim 6 of the patent.

2. Assume that claim 1 of the patent recites, as one of its limitations, limitation W. Assume either that reference XYZ was applied in a rejection during the prior examination of the patent, or that the teachings of reference XYZ are purely cumulative to a reference cited in a rejection during the prior examination of the patent. Assume further that reference ABC teaches that the limitation W would have been either inherent given the teachings of reference XYZ, or would have been obvious in view of the combination of XYZ and ABC. Reference ABC was cited in an information disclosure statement but was never discussed or applied in a rejection ***in combination with the XYZ reference*** during the prior examination of the patent under reexamination. **Requester would state** that reference XYZ was present during the prior examination of the patent under reexamination because it was applied in a rejection during the prosecution of the patent, and that reference ABC was cited in an information disclosure statement but never applied in a rejection (or never discussed), **in combination with the XYZ reference** during the prior examination of the patent under reexamination Requester would then state (1) that the ***combination*** of the XYZ reference and the ABC reference, both of which are cited in the information disclosure statement, contains a teaching of limitation W as recited in claim 1, (2) that this teaching provided by the **combination** of the XYZ and ABC references was not presented during the prior examination of the patent under reexamination, (3) that a reasonable examiner would consider this teaching important in determining whether or not the claims are patentable, and (4) that the presentation of this teaching raises a SNQ with respect to claim 1 of the patent.

Example of a Detailed Explanation

Assume, for example, that a requester believes that the XYZ reference, alone, anticipates claims 1-5. The requester would expressly propose a rejection of claims 1-5 under 35 USC 102(b) as being anticipated by the XYZ reference. In a claim chart, the requester would then show how **each limitation** of claims 1-5 is anticipated by the XYZ reference. If the requester believes that the XYZ reference, in view of the ABC reference, renders obvious claims 6-10, the requester would expressly propose a rejection of claims 6-10 under 35 USC 103 as being obvious over the XYZ reference in view of the ABC reference. In a claim chart, the requester would then show which limitations of claims 6-10 are taught by the XYZ reference, and which limitations of claims 6-10 are taught by the ABC reference. The requester should quote each pertinent teaching in the prior art reference, referencing each quote by page, column and line number, and any relevant figure numbers. Finally, for a proposed rejection, the requester must show how these two references are combined, and the teaching in either the XYZ or the ABC references which provides the motivation to combine these references in order to render claims 6-10 obvious.

REPLACEMENT DOCUMENTS

If the originally-filed PTO/SB/08 (former PTO-1449) or its equivalent lists patents or printed publications that are NOT discussed in at least one proposed rejection or statement identifying an SNQ AND in the corresponding detailed explanation in the originally-filed request, the requester may file a paper containing a **replacement PTO/SB/08 (former PTO-1449) or its equivalent listing ONLY** those patents and printed publications that are so discussed. The replacement PTO/SB/08 or its equivalent should include a cover letter expressly withdrawing from the request any previously cited references that are now being omitted by the replacement PTO/SB/08 or its equivalent. Similarly, **if any patent or printed publication discussed** in at least one proposed rejection or statement identifying an SNQ AND in the corresponding detailed explanation **in the originally-filed request is not listed in the originally-filed PTO/SB/08 (former PTO-1449)** or its equivalent, the requester must file a **replacement PTO/SB/08 (former PTO-1449)** or its equivalent listing **all** of the patents and printed publications, including the previously omitted reference(s), and provide copies of the missing references if copies were not provided with the originally-filed request.

If a copy of a patent, printed publication, or an English-language translation of a patent or printed publication, that is cited in the PTO/SB/08 (former PTO-1449) or its equivalent, is illegible, missing, or incomplete (i.e., it does not contain all of the pages indicated in the PTO/SB/08 (former PTO-1449) or its equivalent), a replacement copy of the patent or printed publication is required.

If a copy of any disclaimer, certificate of correction, or reexamination certificate issued in the patent, or a copy of the entire patent for which reexamination is requested as described in item #6, is missing, or if the copy that was received by the Office was illegible or incomplete, a replacement document (i.e., a replacement copy of the disclaimer, certificate of correction, reexamination certificate, or entire patent under reexamination as described in item #6) is required.

If the requester fails to correctly identify the patent number or the claims for which reexamination is requested on the transmittal form for the request (PTO/SB/57, or an equivalent) as described in item #2, and the patent number and the claims for which reexamination is requested are correctly identified in the originally-filed request, a **replacement transmittal form** is required.

If a certificate of service on the patent owner, as described in item #7, is missing, or if the certificate of service received by the Office is inaccurate or incomplete, a replacement certificate of service is required.

Replacement documents may be facsimile transmitted. A paper containing a replacement statement and explanation may NOT be facsimile transmitted.

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor LARSON, et al.
Filer:	William Neal Hughet/Tamika Miles
Attorney Docket Number:	3755-121

Filed as Large Entity

inter partes reexam Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Request for inter reexamination	1813	1	8800	8800
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**8800**

Electronic Acknowledgement Receipt	
EFS ID:	6519927
Application Number:	95001270
International Application Number:	
Confirmation Number:	2128
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor LARSON, et al.
Customer Number:	06449
Filer:	William Neal Hughet/Tamika Miles
Filer Authorized By:	William Neal Hughet
Attorney Docket Number:	3755-121
Receipt Date:	25-NOV-2009
Filing Date:	
Time Stamp:	17:51:00
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$8800
RAM confirmation Number	3597
Deposit Account	022135
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	
Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)	
Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees) Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees) Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)					
File Listing:					
Document Number	**Document Description**	**File Name**	**File Size(Bytes)/ Message Digest**	**Multi Part /.zip**	**Pages (if appl.)**
1	NPL Documents	Exhibit1Larson.pdf	4244893 9bd0e67b2e268c2444f2f3b8b819cdb5dcd979e28	no	74
Warnings:					
Information:					
2	NPL Documents	Exhibit2AventailConnectAdminGuide31.pdf	622865 8e0ec55b403a13f5f3b321f17abb32c242b273f	no	125
Warnings:					
Information:					
3	NPL Documents	Exhibit3VirtualPrivateNetworkingAnOverview.pdf	1149224 0242545ea19a2e1f8b865473eb8b1e7e7a9cca	no	28
Warnings:					
Information:					
4	NPL Documents	Exhibit4RFC1035.pdf	98259 13c7f893ac473d680fccd3b39ca193a76bc0fdd4	no	56
Warnings:					
Information:					
5	NPL Documents	Exhibit7GalvinPublicKeyDistributionwithSecure.pdf	956965 602f474067b8e266fa74f8a84d6b36277b05f998	no	12
Warnings:					
Information:					
6	NPL Documents	Exhibit8aGauntletFirewallforWindowsNTAdmin.pdf	21350755 603d7d4c94c2fb6cd62cf72a521c1fc31bc05f2d	no	138
Warnings:					
Information:					
7	NPL Documents	Exhibit10InstallingConfiguringandUsingPPTP.pdf	2428789 ed4bda17a68b292551aa9ba20fc23c12a55b7784	no	30
Warnings:					
Information:					
8	NPL Documents	Exhibit11BuildingaMicrosoftVPNAComprehensiveCollection.pdf	23764386 09d5448aaaf273a32e9a700acd0c3ae32db361cd	no	216

Warnings:					
Information:					
9	NPL Documents	Exhibit14NoticeofAllowance486.pdf	438608 a0a9aa7f4202dbb95770dc7e1695bf1e62811314	no	10
Warnings:					
Information:					
10	NPL Documents	Exhibit9.pdf	8264306 52cef7cb87ca2651a9425e80c16cb85e60a331563	no	106
Warnings:					
Information:					
11	NPL Documents	Exhibit8bGauntletFirewallforWindowsNTAdmin.pdf	19719372 9f500a7358d6651b568daffbeb0db7395e4c8011	no	139
Warnings:					
Information:					
12	NPL Documents	Exhibit5BuildingaMicrosoftVPN.pdf	23778793 6afa8859648b9f937918db9b3ba53878cad03d677	no	216
Warnings:					
Information:					
13	NPL Documents	Exhibit5KoslurBuildingandManagingVPNs2.pdf	11662304 01e8a5135bc2b9410b12190ae760051 7b9a307b8	no	180
Warnings:					
Information:					
14	NPL Documents	Exhibit6KaufmanImplementingIPsec1.pdf	14401558 11d6956b09fad26a55c1c03c51632d04b25884d7	no	200
Warnings:					
Information:					
15	NPL Documents	Exhibit6KaufmanImplementingIPsec2.pdf	10427650 /55.3db/9aed304dab3594c4c40a3212131 9c541f1	no	80
Warnings:					
Information:					
16	NPL Documents	Exhibit12SBO8.pdf	296349 14dd8219880564aae1cad7cf6406725280 8a0d3	no	5
Warnings:					
Information:					
17	NPL Documents	Exhibit13ClaimConstructionOrder.pdf	3809824 e1502a14d91261820fd2e8abf322fbe320aa2284	no	36

Warnings:					
Information:					
18	NPL Documents	AppA180ClaimChartAventail.pdf	3372015 a81cfEbd0891c6dc2a198a36fc6b378e4B3b5480	no	37
Warnings:					
Information:					
19	NPL Documents	AppB180ClaimChartVPNOverviewRFC1035.pdf	3070716 3e4fcf5fc7c25442ed9858cad77fba3164baec5b0	no	38
Warnings:					
Information:					
20	NPL Documents	AppC180ClaimChartKosiur.pdf	2040813 bv0ea6cdb8fbfbe1bd18/b66b15a0bf25ee13388a	no	24
Warnings:					
Information:					
21	NPL Documents	AppD180ClaimChartKaufman.pdf	2284985 c6b8419c4134e7d48d4be503fbfe53e89f1c3f3c	no	24
Warnings:					
Information:					
22	NPL Documents	AppE180ClaimChartKaufmanGalvin.pdf	2350205 d78a6d5d1d1b4dfd518f3725599f1e02f80d9e271b1	no	35
Warnings:					
Information:					
23	NPL Documents	AppF180ClaimChartGauntlet.pdf	2046277 d4de413ae130c4409bLd38a53f332ec6188	no	31
Warnings:					
Information:					
24	NPL Documents	AppG180ClaimChartHandsOnInstallingNT.pdf	2561466 190f81e55c8827558Jda6b1e32bdc4J211b11aed	no	23
Warnings:					
Information:					
25	NPL Documents	AppH180ClaimChartMicrosoftVPN.pdf	872923 211f7dcf3a67f25c78881238103cd1c9917865f	no	20
Warnings:					
Information:					
26	Receipt of Original Inter Partes Reexam Request	Reqforreexam180patent.pdf	6348049 81f78dac17c45e540901a7ed094ec7a925cb14a9	no	53

Warnings:					
Information:					
27	Miscellaneous Incoming Letter	121CertificateofServices.pdf	150623 74c37d117c3d17145d9986ced73a8cfb85079985	no	3
Warnings:					
Information:					
28	Fee Worksheet (PTO-875)	fee-info.pdf	30065 f864f7395f4d4325244f74b6b6a8070b905ad6f2	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	172543037		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Request for Reexamination of 7,188,180

Exhibit 1

U.S. Patent No. 7,188,180

US007188180B2

(12) **United States Patent**
Larson et al.

(10) **Patent No.: US 7,188,180 B2**
(45) **Date of Patent: Mar. 6, 2007**

(54) **METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK**

(75) Inventors: **Victor Larson**, Fairfax, VA (US); **Robert Durham Short, III**, Leesburg, VA (US); **Edmund Colby Munger**, Crownsville, MD (US); **Michael Williamson**, South Riding, VA (US)

(73) Assignee: **VimetX, Inc.**, Scotts Valley, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 413 days.

(21) Appl. No.: **10/702,486**

(22) Filed: **Nov. 7, 2003**

(65) **Prior Publication Data**

US 2004/0107285 A1 Jun. 3, 2004

Related U.S. Application Data

(60) Division of application No. 09/558,209, filed on Apr. 26, 2000, now abandoned, which is a continuation-in-part of application No. 09/504,783, filed on Feb. 15, 2000, now Pat. No. 6,502,135, which is a continuation-in-part of application No. 09/429,643, filed on Oct. 29, 1999, now Pat. No. 7,010,604.

(60) Provisional application No. 60/137,704, filed on Jun. 7, 1999, provisional application No. 60/106,261, filed on Oct. 30, 1998.

(51) **Int. Cl.**
G06F 15/173 (2006.01)

(52) **U.S. Cl.** **709/227**; 709/228

(58) **Field of Classification Search** 709/225–229, 709/245

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,933,846	A	6/1990	Humphrey et al.
5,341,426	A	8/1994	Barney et al.
5,588,060	A	12/1996	Aziz
5,689,566	A	11/1997	Nguyen

(Continued)

FOREIGN PATENT DOCUMENTS

DE	199 24 575	12/1999

(Continued)

OTHER PUBLICATIONS

Search Report (dated Jun. 18, 2002), International Application No. PCT/US01/13260.

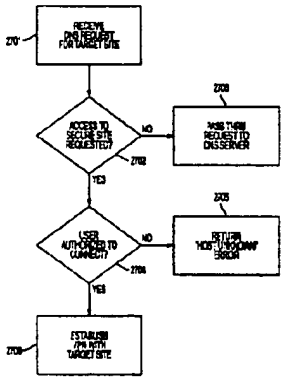
(Continued)

Primary Examiner—Krisna Lim
(74) *Attorney, Agent, or Firm*—Banner & Witcoff, Ltd.

(57) **ABSTRACT**

A technique is disclosed for establishing a secure communication link between a first computer and a second computer over a computer network. Initially, a secure communication mode of communication is enabled at a first computer without a user entering any cryptographic information for establishing the secure communication mode of communication. Then, a secure communication link is established between the first computer and a second computer over a computer network based on the enabled secure communication mode of communication. The secure communication link is a virtual private network communication link over the computer network in which one or more data values that vary according to a pseudo-random sequence are inserted into each data packet.

41 Claims, 40 Drawing Sheets



U.S. PATENT DOCUMENTS

5,787,172	A		7/1998	Arnold
5,796,942	A		8/1998	Esbensen
5,805,801	A		9/1998	Holloway et al.
5,842,040	A		11/1998	Hughes et al.
5,870,610	A		2/1999	Beyda et al.
5,878,231	A		3/1999	Baehr et al.
5,892,903	A		4/1999	Klaus
5,898,830	A		4/1999	Wesinger, Jr. et al.
5,905,859	A		5/1999	Holloway et al.
6,006,259	A		12/1999	Adelman et al.
6,016,318	A		1/2000	Tomoike
6,052,788	A		4/2000	Wesinger, Jr. et al.
6,079,020	A		6/2000	Liu
6,092,200	A		7/2000	Muniyappa et al.
6,119,171	A	*	9/2000	Alkhatib 709/245
6,119,234	A	*	9/2000	Aziz et al. 726/11
6,158,011	A		12/2000	Chen et al.
6,178,409	B1		1/2001	Weber et al.
6,178,505	B1		1/2001	Schneider et al.
6,226,751	B1		5/2001	Arrow et al.
6,243,749	B1		6/2001	Sitaraman et al.
6,256,671	B1	*	7/2001	Strentzsch et al. 709/227
6,286,047	B1		9/2001	Ramanathan et al.
6,330,562	B1		12/2001	Boden et al.
6,332,158	B1		12/2001	Risley et al.
6,353,614	B1		3/2002	Borella et al.

FOREIGN PATENT DOCUMENTS

EP	0 814 589		12/1997
EP	0 814 589	A	12/1997
EP	0 838 930		4/1998
EP	0 838 930	A	4/1998
EP	0 858 189		8/1998
GB	2 317 792		4/1998
GB	2 317 792	A	4/1998
GB	2 334 181	A	8/1999
WO	9827783	A	6/1998
WO	WO 98/27783		6/1998
WO	WO 98 55930		12/1998
WO	WO 98 59470		12/1998
WO	WO 99 38081		7/1999
WO	WO 99 48303		9/1999
WO	WO 01 50688		7/2001

OTHER PUBLICATIONS

Search Report (dated Jun. 28, 2002), International Application No. PCT/US01/13261.

Donald E. Eastlake, "Domain Name System Security Extensions", DNS Security Working Group, Apr. 1998, 51 pages.

D. B. Chapman et al., "Building Internet Firewalls", Nov. 1995, pp. 278-297 and pp. 351-375.

P. Srisuresh et al., "DNS extensions to Network Address Translators", Jul. 1998, 27 pages.

Laurie Wells. "Security Icon", Oct. 19, 1998. 1 page.

W. Stallings, "Cryptography And Network Security", 2nd Edition, Chapter 13, IP Security, Jun. 8, 1998, pp. 399-440.

W. Stallings, "New Cryptography and Network Security Book", Jun. 8, 1998, 3 pages.

Fasbender, Kesdogan, and Kubitz: "Variable and Scalable Security: Protection of Location Information in Mobile IP", IEEE publication. 1996. pp. 963-967.

Search Report (dated Aug. 20, 2002), International Application No. PCT/US01/04340.

Search Report (dated Aug. 23, 2002), International Application No. PCT/US01/13260.

Shree Murthy et al., "Congestion-Oriented Shortest Multipath Routing", Proceedings of IEEE INFOCOM, 1996, pp. 1028-1036.

Jim Jones et al., "Distributed Denial of Service Attacks: Defenses", Global Integrity Corporation, 2000, pp. 1-14.

James E. Bellaire, "New Statement of Rules—Naming Internet Domains", Internet Newsgroup, Jul. 30, 1995, 1 page.

D. Clark, "US Calls for Private Domain-Name System", Computer, IEEE Computer Society, Aug. 1, 1998, pp. 22-25.

August Bequai, "Balancing Legal Concerns Over Crime and Security in Cyberspace", Computer & Security, vol. 17, No. 4, 1998, pp. 293-298.

Rich Winkel, "CAQ: Networking With Spooks: The NET & The Control Of Information", Internet Newsgroup, Jun. 21, 1997, 4 pages.

Linux FreeS/WAN Index File, printed from http://liberty.freeswan.org/freeswan_trees/freeswan-1.3/doc/on Feb. 21, 2002, 3 Pages.

J. Gilmore, "Swan: Securing the Internet against Wiretapping", printed from http://liberty.freeswan.org/freeswan_trees/freeswan-1.3/doc/rationale.html on Feb. 21, 2002, 4 pages.

Glossary for the Linux FreeS/WAN project, printed from http://liberty.freeswan.org/freeswan_trees/freeswan-1.3/doc/glossary.html on Feb. 21, 2002, 25 pages.

Alan O. Frier et al., "The SSL Protocol Version 3.0", Nov. 18, 1996, printed from http://www.netscape.com/eng/ss13/draft302.txt on Feb. 4, 2002, 56 pages.

Search Report (dated Oct. 7, 2002), International Application No. PCT/US01/13261.

F. Halsall, "Data Communications, Computer Networks And Open Systems", Chapter 4, Protocol Basics, 1996, pp. 198-203.

Reiter, Michael K. and Rubin, Aviel D. (AT&T Labs—Research), "Crowds: Anonymity for Web Transmission", pp. 1-23.

Dolev, Shlomi and Ostrovsky, Rafil, "Efficient Anonymous Multicast and Reception" (Extended Abstract), 16 pages.

Rubin, Aviel D., Greer, Daniel, and Ranum, Marcus J. (Wiley Computer Publishing), "Web Security Sourcebook", pp. 82-94.

Fasbender, Kesdogan, and Kubitz: "Variable and Scalable Security" Protection of Location Information in Mobile IP, IEEE publication, 1996, pp. 963-967.

Laurie Wells (LANCASTERDIBELMAIL MSN COM); "Subject: Security Icon" USENET Newsgroup, Oct. 19, 1998, XP002200606.

Davila J et al, "Implementation of Virtual Private Networks at the Transport Layer", Information Security, Second International Workshop. ISW'99. Proceedings (Lecture Springer-Verlag Berlin, Germany, [Online] 1999, pp. 85-102, XP002399276, ISBN 3-540-66695-B, retrieved from the Internet: URL: http://www.springerlink.com/content/4uac0tb0hecoma89/fulltext.pdf> (Abstract).

* cited by examiner

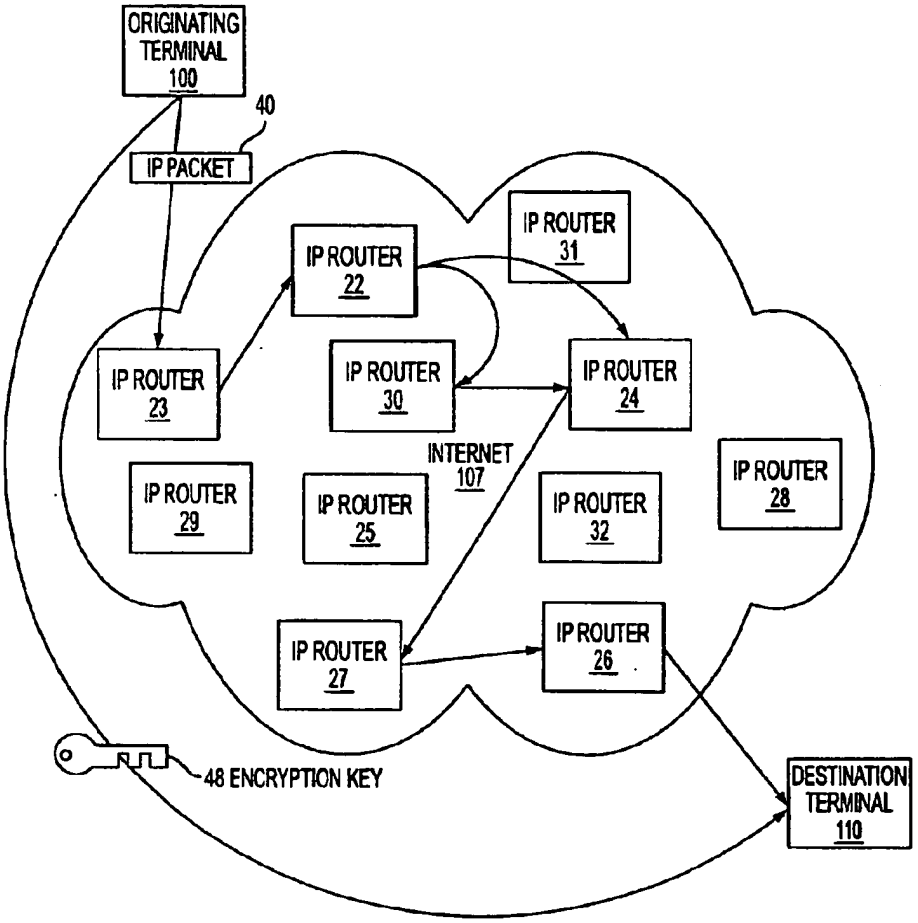

ORIGINATING TERMINAL 100
40
IP PACKET
IP ROUTER 22
IP ROUTER 31
IP ROUTER 23
IP ROUTER 30
IP ROUTER 24
INTERNET 107
IP ROUTER 29
IP ROUTER 25
IP ROUTER 32
IP ROUTER 28
IP ROUTER 27
IP ROUTER 26
48 ENCRYPTION KEY
DESTINATION TERMINAL 110

FIG. 1

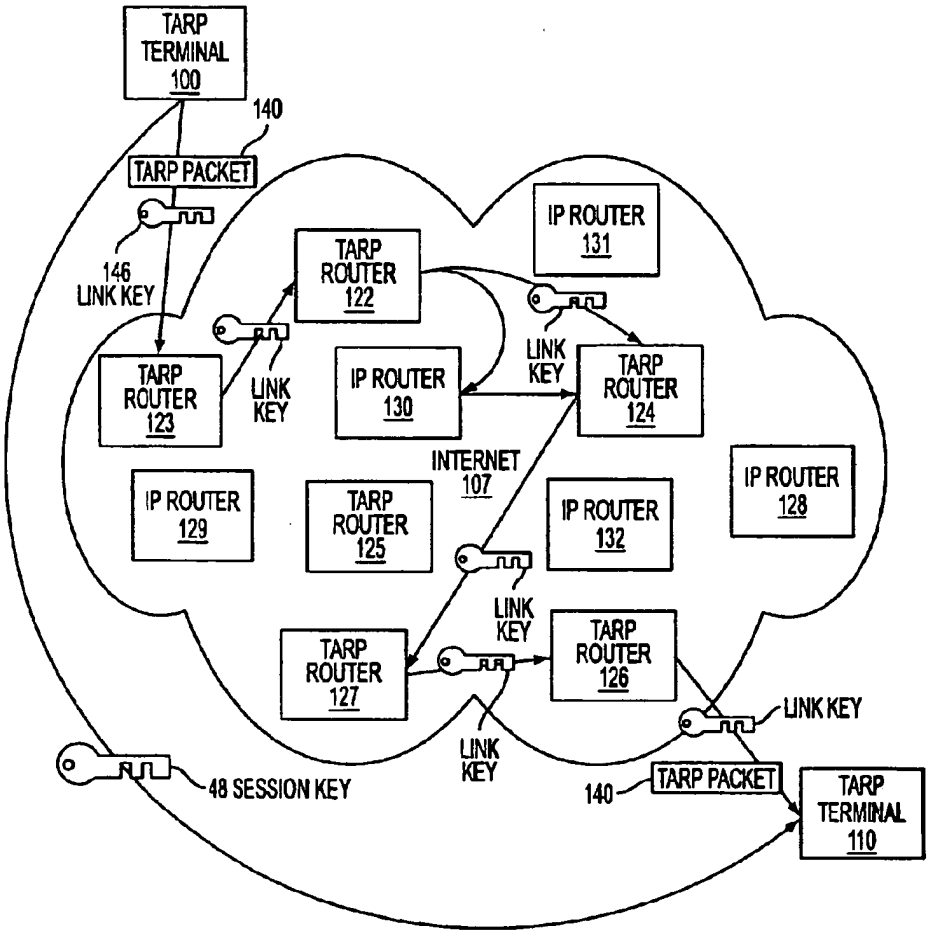

TARP TERMINAL 100
140
TARP PACKET
146 LINK KEY
TARP ROUTER 122
IP ROUTER 131
LINK KEY
TARP ROUTER 123
LINK KEY
IP ROUTER 130
TARP ROUTER 124
INTERNET 107
IP ROUTER 129
TARP ROUTER 125
IP ROUTER 132
IP ROUTER 128
LINK KEY
TARP ROUTER 127
TARP ROUTER 126
LINK KEY
LINK KEY
48 SESSION KEY
140
TARP PACKET
TARP TERMINAL 110

FIG. 2

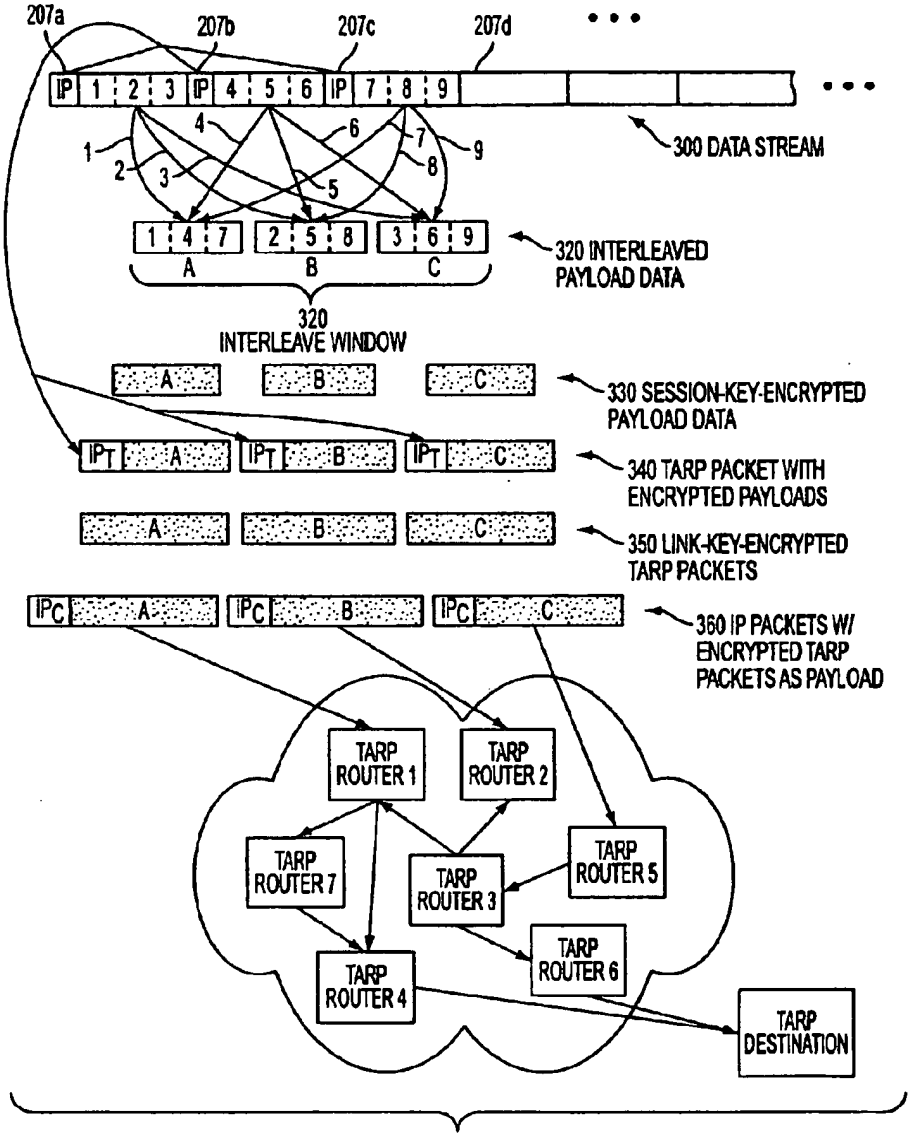

207a
207b
207c
207d
IP 1 2 3 IP 4 5 6 IP 7 8 9
300 DATA STREAM
1 4 7
2 5 8
3 6 9
A
B
C
320 INTERLEAVED PAYLOAD DATA
320 INTERLEAVE WINDOW
330 SESSION-KEY-ENCRYPTED PAYLOAD DATA
IPT A IPT B IPT C
340 TARP PACKET WITH ENCRYPTED PAYLOADS
350 LINK-KEY-ENCRYPTED TARP PACKETS
IPC A IPC B IPC C
360 IP PACKETS W/ ENCRYPTED TARP PACKETS AS PAYLOAD
TARP ROUTER 1
TARP ROUTER 2
TARP ROUTER 7
TARP ROUTER 3
TARP ROUTER 5
TARP ROUTER 6
TARP ROUTER 4
TARP DESTINATION

FIG. 3A

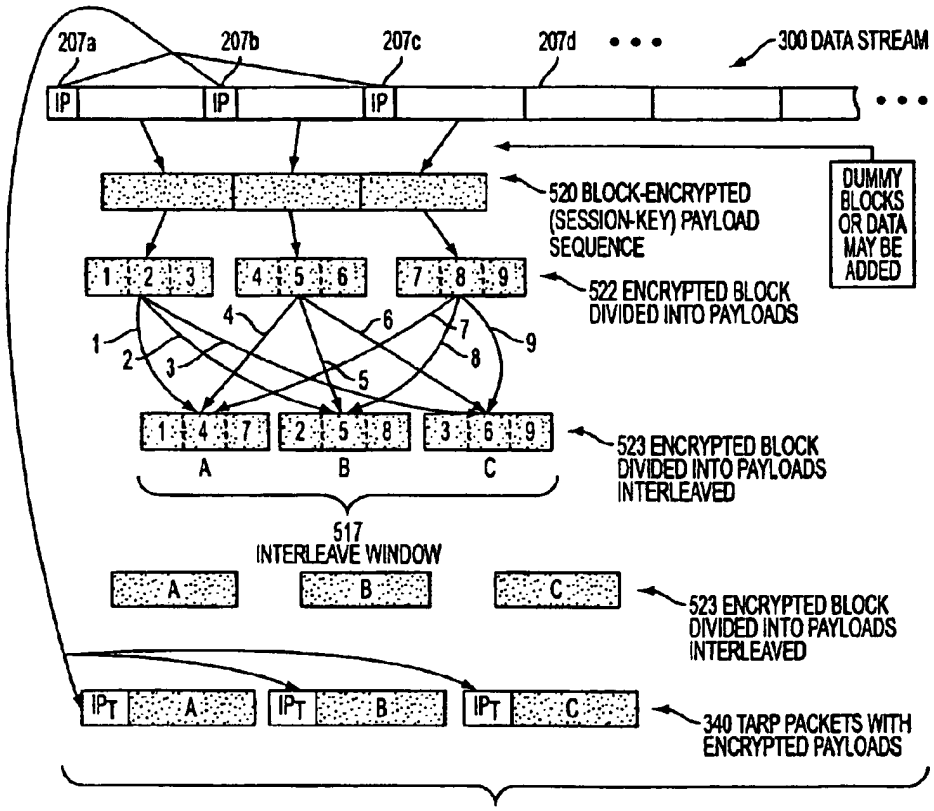

207a
207b
207c
207d
300 DATA STREAM
IP
520 BLOCK-ENCRYPTED (SESSION-KEY) PAYLOAD SEQUENCE
DUMMY BLOCKS OR DATA MAY BE ADDED
522 ENCRYPTED BLOCK DIVIDED INTO PAYLOADS
523 ENCRYPTED BLOCK DIVIDED INTO PAYLOADS INTERLEAVED
A
B
C
517
INTERLEAVE WINDOW
IPT
340 TARP PACKETS WITH ENCRYPTED PAYLOADS

FIG. 3B

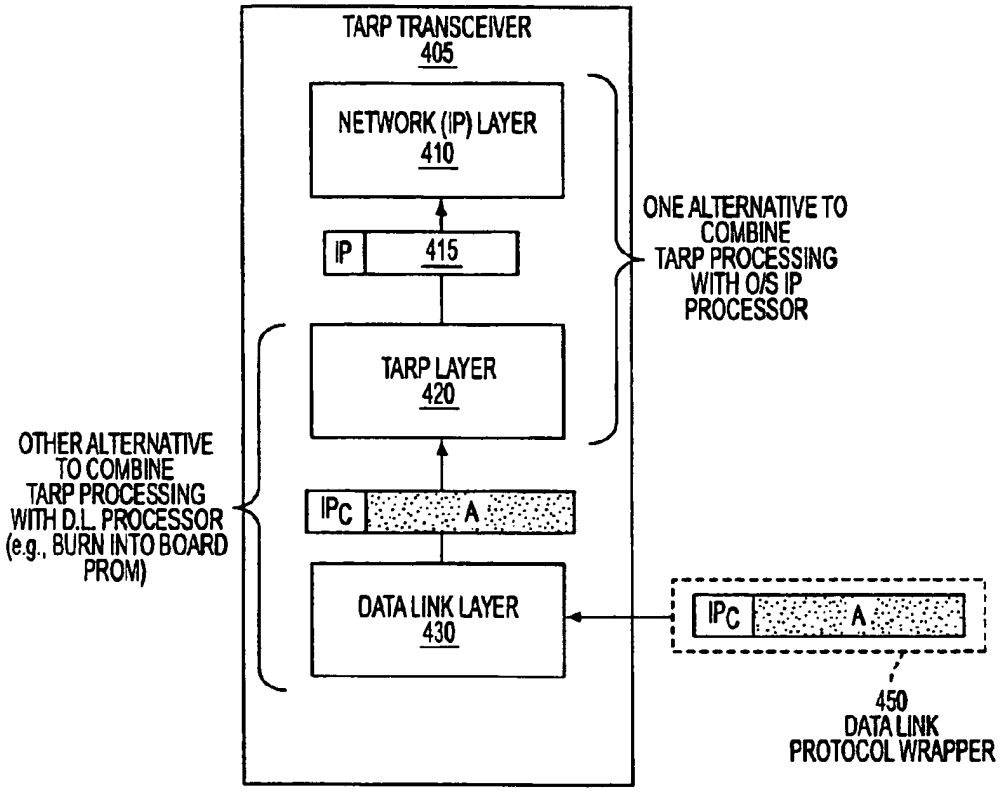

TARP TRANSCEIVER
405
NETWORK (IP) LAYER
410
IP
415
TARP LAYER
420
IPC
A
DATA LINK LAYER
430
ONE ALTERNATIVE TO COMBINE TARP PROCESSING WITH O/S IP PROCESSOR
OTHER ALTERNATIVE TO COMBINE TARP PROCESSING WITH D.L. PROCESSOR (e.g., BURN INTO BOARD PROM)
IPC
A
450
DATA LINK PROTOCOL WRAPPER

FIG. 4

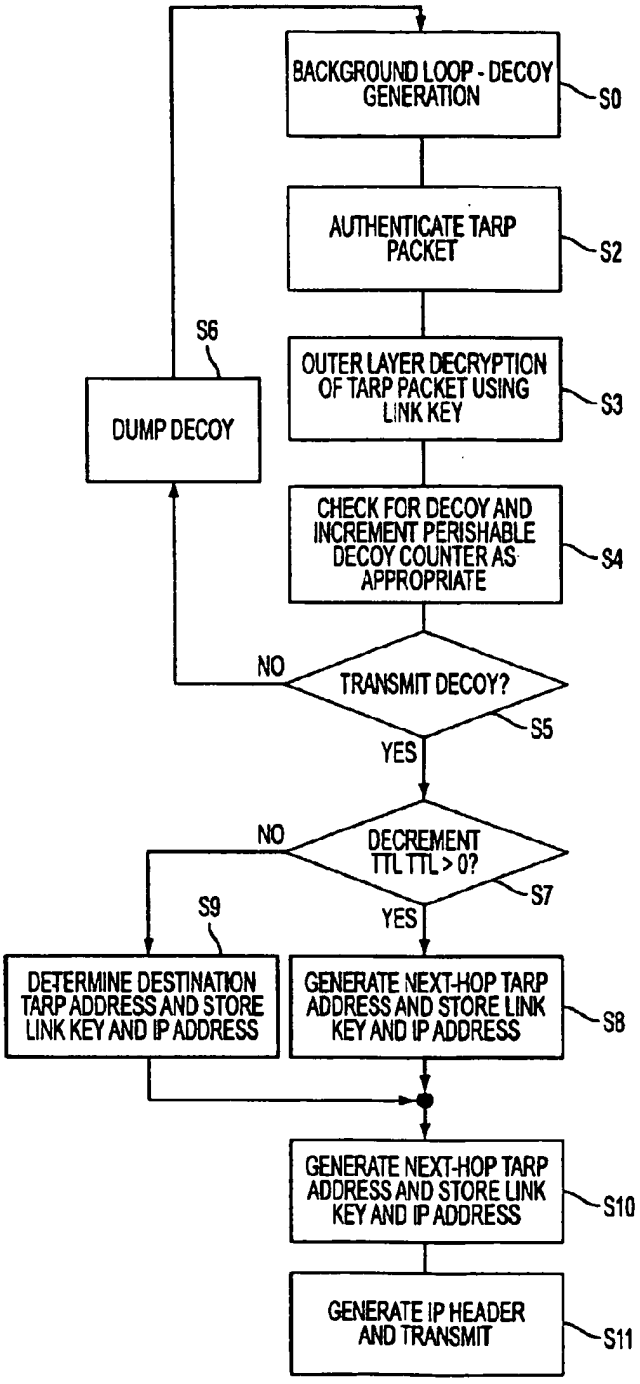

BACKGROUND LOOP - DECOY GENERATION
S0
AUTHENTICATE TARP PACKET
S2
OUTER LAYER DECRYPTION OF TARP PACKET USING LINK KEY
S3
CHECK FOR DECOY AND INCREMENT PERISHABLE DECOY COUNTER AS APPROPRIATE
S4
TRANSMIT DECOY?
S5
NO
YES
DUMP DECOY
S6
DECREMENT TTL TTL > 0?
S7
NO
YES
S9
DETERMINE DESTINATION TARP ADDRESS AND STORE LINK KEY AND IP ADDRESS
GENERATE NEXT-HOP TARP ADDRESS AND STORE LINK KEY AND IP ADDRESS
S8
GENERATE NEXT-HOP TARP ADDRESS AND STORE LINK KEY AND IP ADDRESS
S10
GENERATE IP HEADER AND TRANSMIT
S11

FIG. 5

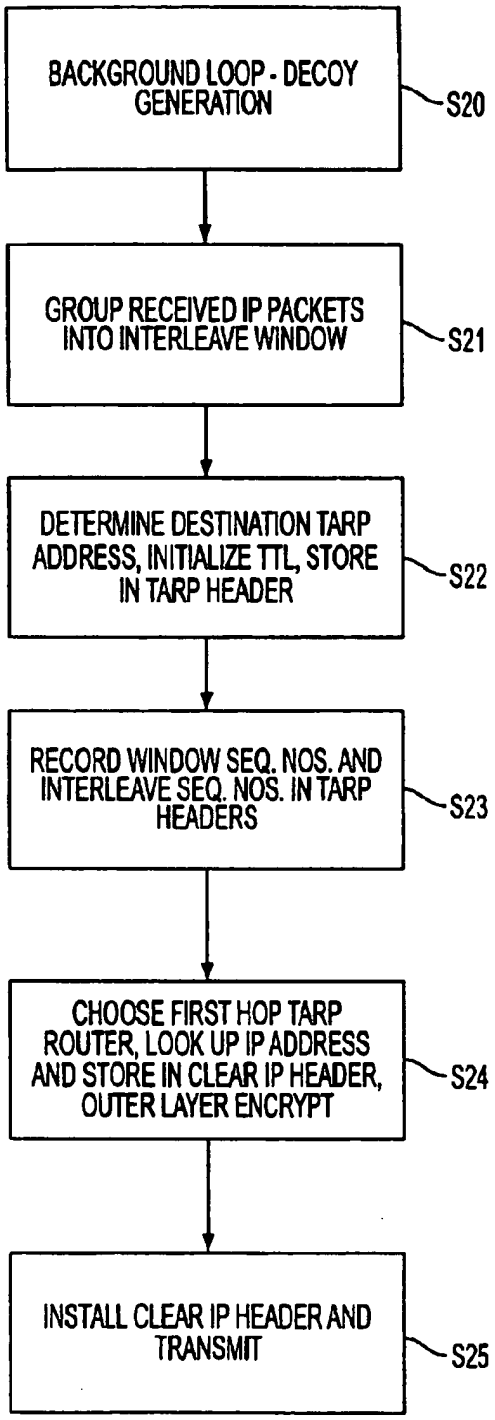

BACKGROUND LOOP - DECOY GENERATION
S20
GROUP RECEIVED IP PACKETS INTO INTERLEAVE WINDOW
S21
DETERMINE DESTINATION TARP ADDRESS, INITIALIZE TTL, STORE IN TARP HEADER
S22
RECORD WINDOW SEQ. NOS. AND INTERLEAVE SEQ. NOS. IN TARP HEADERS
S23
CHOOSE FIRST HOP TARP ROUTER, LOOK UP IP ADDRESS AND STORE IN CLEAR IP HEADER, OUTER LAYER ENCRYPT
S24
INSTALL CLEAR IP HEADER AND TRANSMIT
S25

FIG. 6

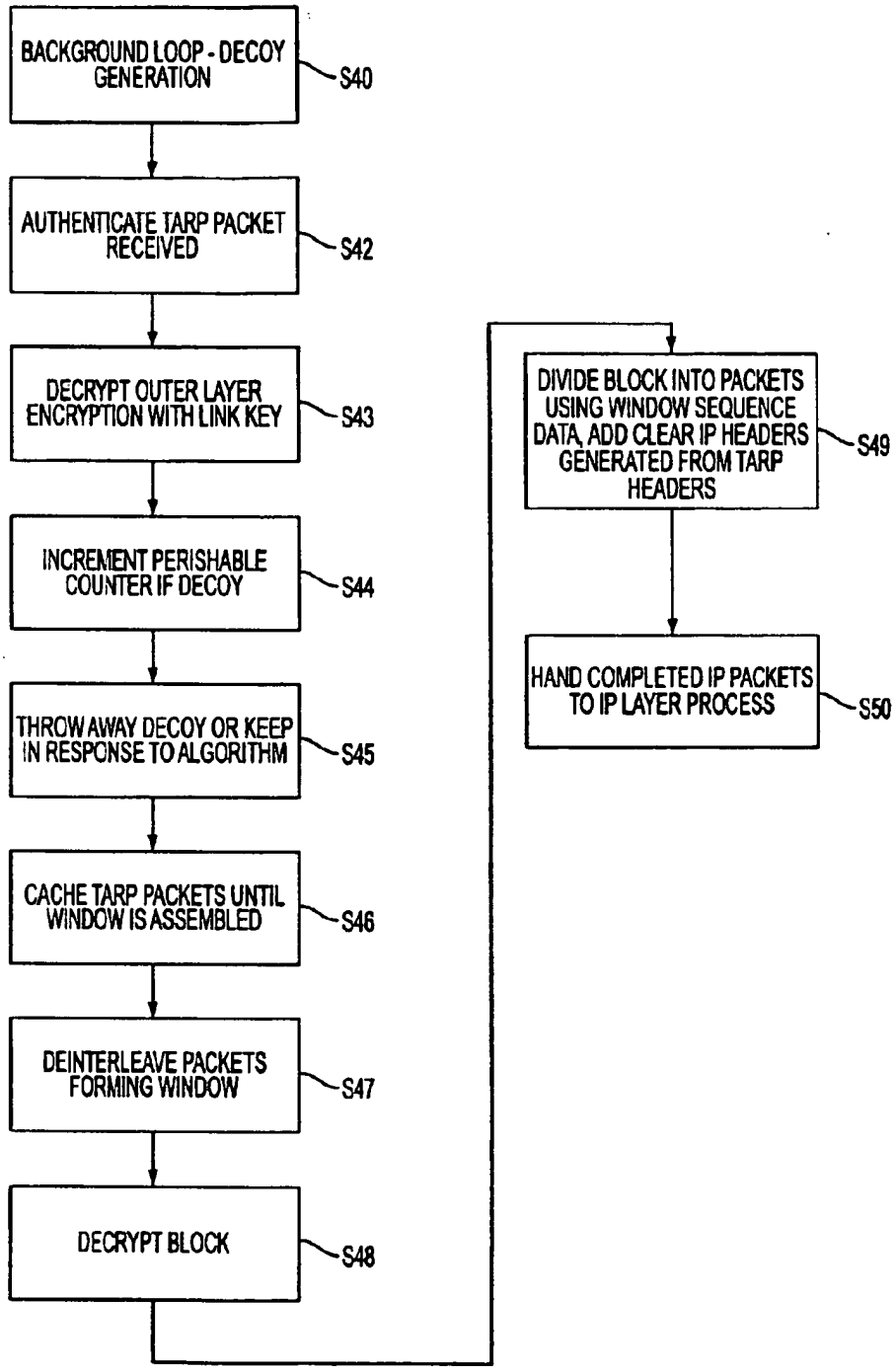

BACKGROUND LOOP - DECOY GENERATION
S40
AUTHENTICATE TARP PACKET RECEIVED
S42
DECRYPT OUTER LAYER ENCRYPTION WITH LINK KEY
S43
INCREMENT PERISHABLE COUNTER IF DECOY
S44
THROW AWAY DECOY OR KEEP IN RESPONSE TO ALGORITHM
S45
CACHE TARP PACKETS UNTIL WINDOW IS ASSEMBLED
S46
DEINTERLEAVE PACKETS FORMING WINDOW
S47
DECRYPT BLOCK
S48
DIVIDE BLOCK INTO PACKETS USING WINDOW SEQUENCE DATA, ADD CLEAR IP HEADERS GENERATED FROM TARP HEADERS
S49
HAND COMPLETED IP PACKETS TO IP LAYER PROCESS
S50

FIG. 7

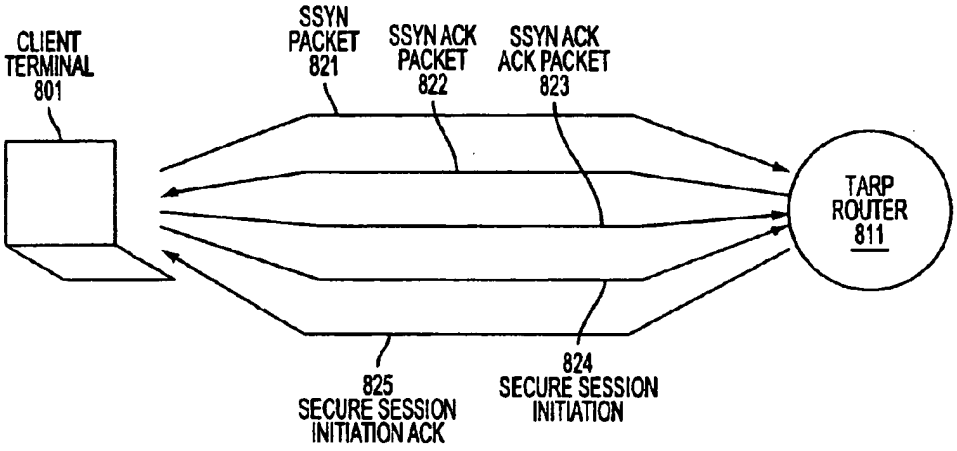

CLIENT TERMINAL 801
SSYN PACKET 821
SSYN ACK PACKET 822
SSYN ACK ACK PACKET 823
TARP ROUTER 811
825 SECURE SESSION INITIATION ACK
824 SECURE SESSION INITIATION

FIG. 8

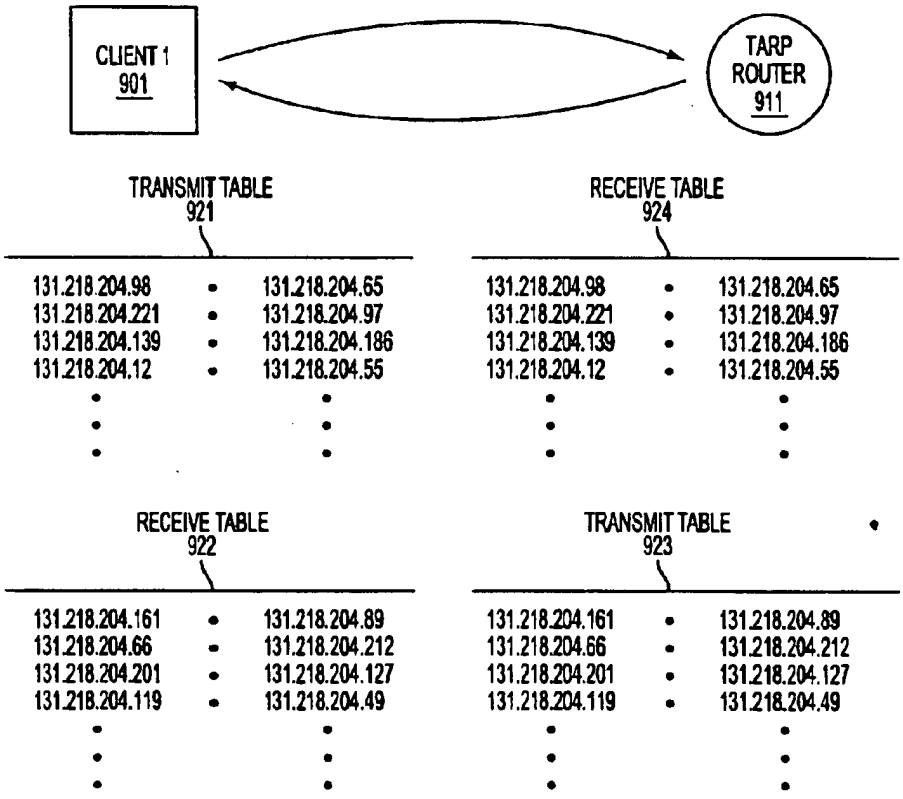

CLIENT 1
901
TARP
ROUTER
911
TRANSMIT TABLE
921
131.218.204.98 • 131.218.204.65
131.218.204.221 • 131.218.204.97
131.218.204.139 • 131.218.204.186
131.218.204.12 • 131.218.204.55
RECEIVE TABLE
924
131.218.204.98 • 131.218.204.65
131.218.204.221 • 131.218.204.97
131.218.204.139 • 131.218.204.186
131.218.204.12 • 131.218.204.55
RECEIVE TABLE
922
131.218.204.161 • 131.218.204.89
131.218.204.66 • 131.218.204.212
131.218.204.201 • 131.218.204.127
131.218.204.119 • 131.218.204.49
TRANSMIT TABLE
923
131.218.204.161 • 131.218.204.89
131.218.204.66 • 131.218.204.212
131.218.204.201 • 131.218.204.127
131.218.204.119 • 131.218.204.49

FIG. 9

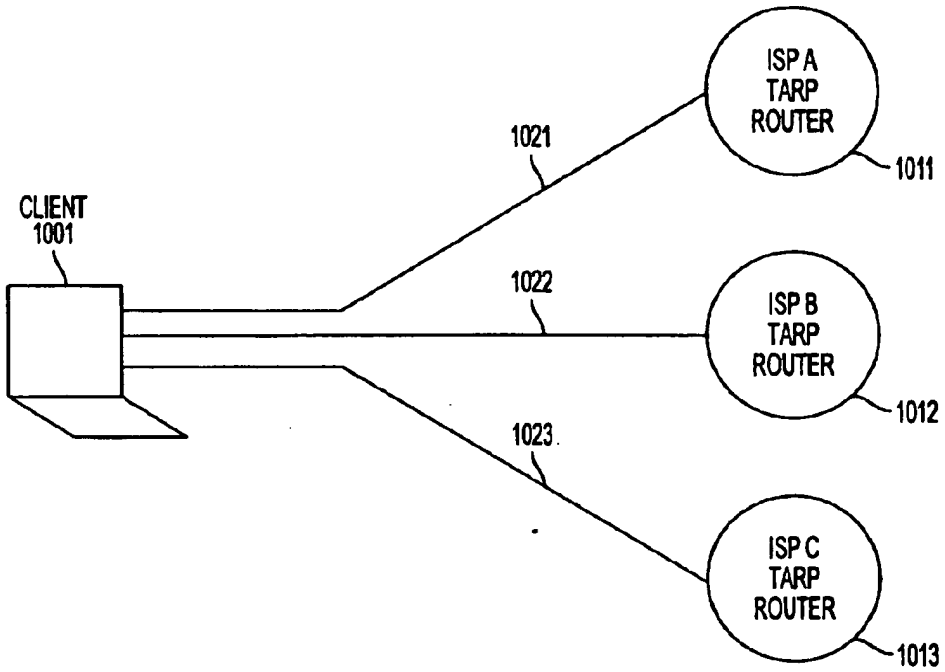

ISP A
TARP
ROUTER
1011
1021
CLIENT
1001
1022
ISP B
TARP
ROUTER
1012
1023
ISP C
TARP
ROUTER
1013

FIG. 10

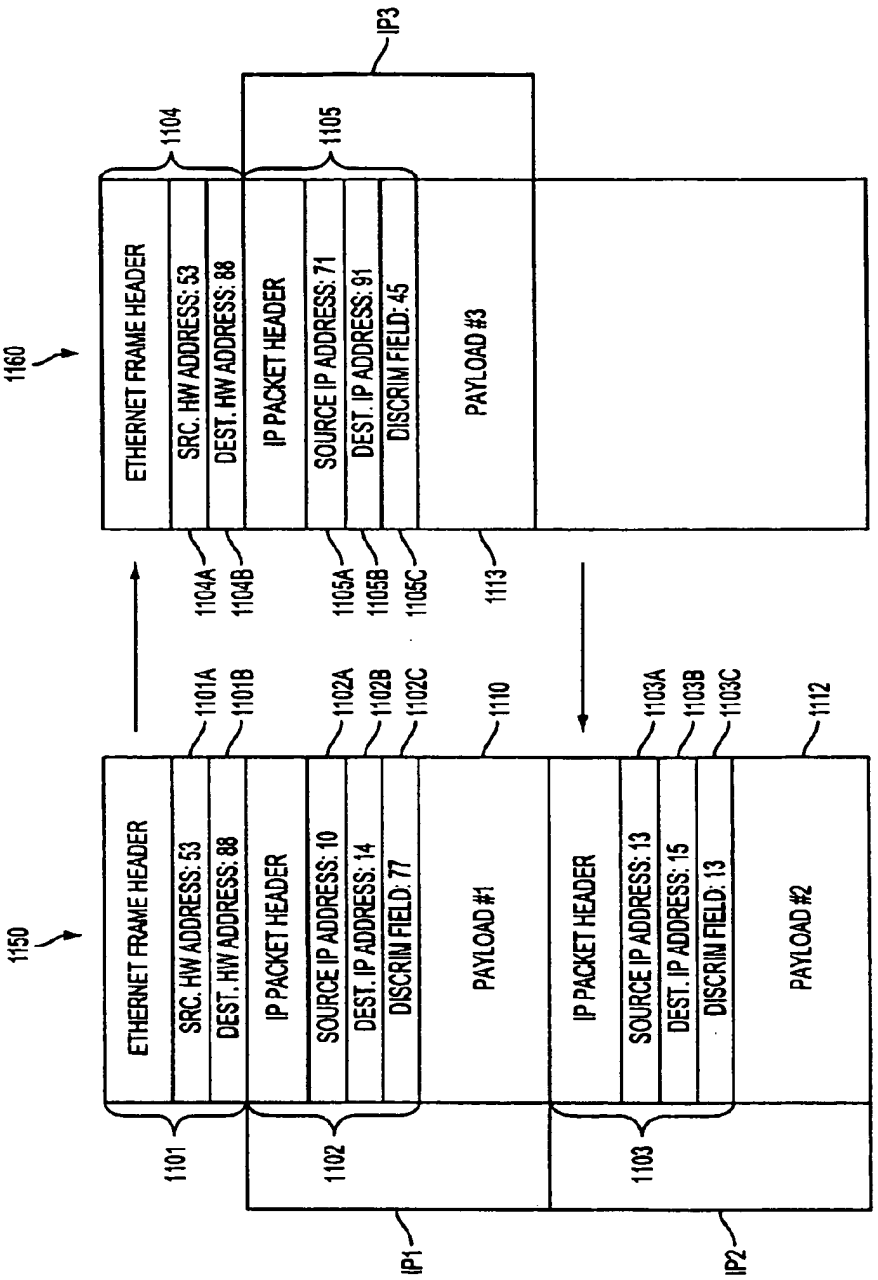

1160
ETHERNET FRAME HEADER
SRC. HW ADDRESS: 53
DEST. HW ADDRESS: 88
IP PACKET HEADER
SOURCE IP ADDRESS: 71
DEST. IP ADDRESS: 91
DISCRIM FIELD: 45
PAYLOAD #3
IP3
1104
1105
1104A
1104B
1105A
1105B
1105C
1113
1150
1101A
1101B
1102A
1102B
1102C
1110
1103A
1103B
1103C
1112
SRC. HW ADDRESS: 53
DEST. HW ADDRESS: 88
SOURCE IP ADDRESS: 10
DEST. IP ADDRESS: 14
DISCRIM FIELD: 77
PAYLOAD #1
IP PACKET HEADER
SOURCE IP ADDRESS: 13
DEST. IP ADDRESS: 15
DISCRIM FIELD: 13
PAYLOAD #2
1101
1102
1103
IP1
IP2

FIG. 11

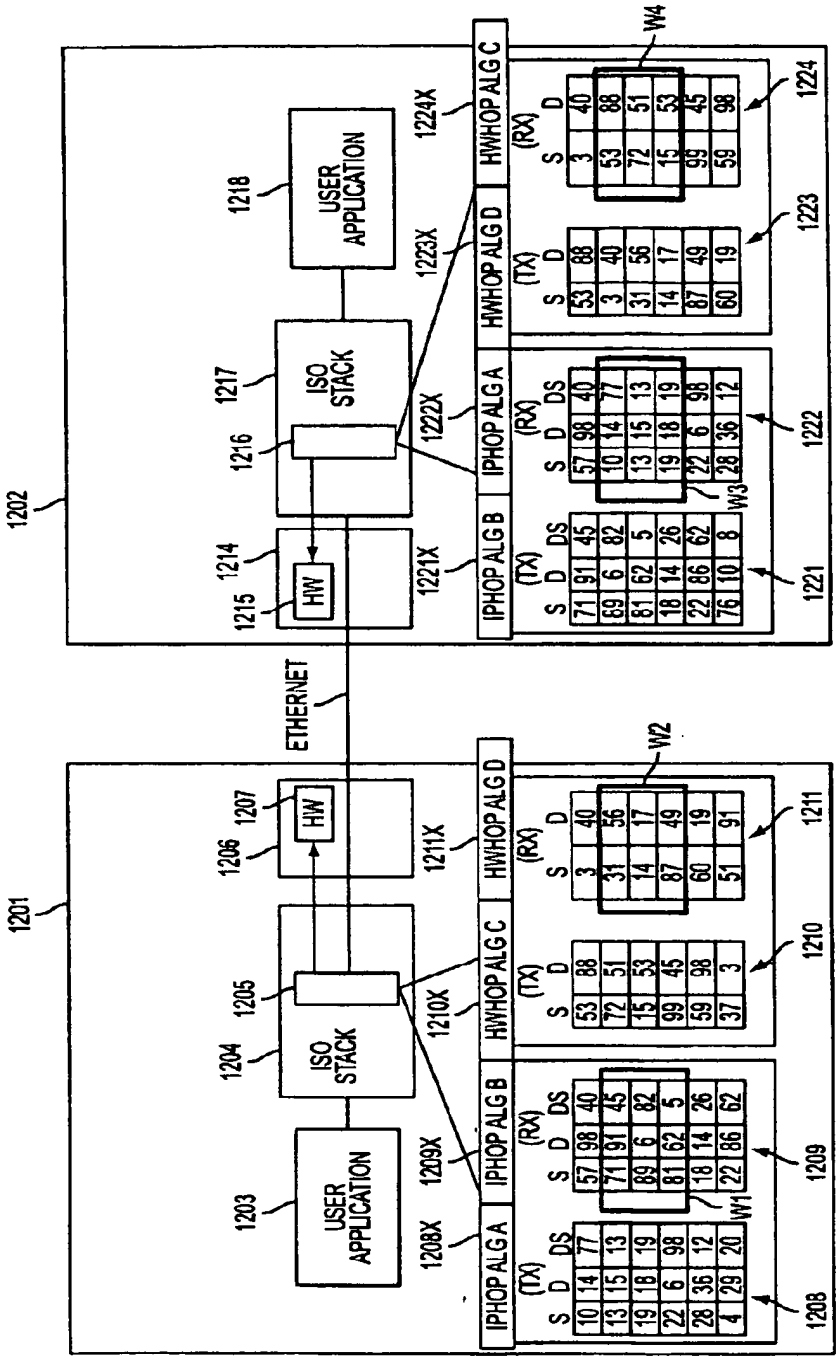

1201
1202
ETHERNET
USER APPLICATION
ISO STACK
HW
IPHOP ALG A
IPHOP ALG B
HWHOP ALG C
HWHOP ALG D
(TX)
(RX)
S
D
DS
W1
W2
W3
W4

FIG. 12A

MODE OR EMBODIMENT	HARDWARE ADDRESSES	IP ADDRESSES	DISCRIMINATOR FIELD VALUES
1. PROMISCUOUS	SAME FOR ALL NODES OR COMPLETELY RANDOM	CAN BE VARIED IN SYNC	CAN BE VARIED IN SYNC
2. PROMISCUOUS PER VPN	FIXED FOR EACH VPN	CAN BE VARIED IN SYNC	CAN BE VARIED IN SYNC
3. HARDWARE HOPPING	CAN BE VARIED IN SYNC	CAN BE VARIED IN SYNC	CAN BE VARIED IN SYNC

FIG. 12B

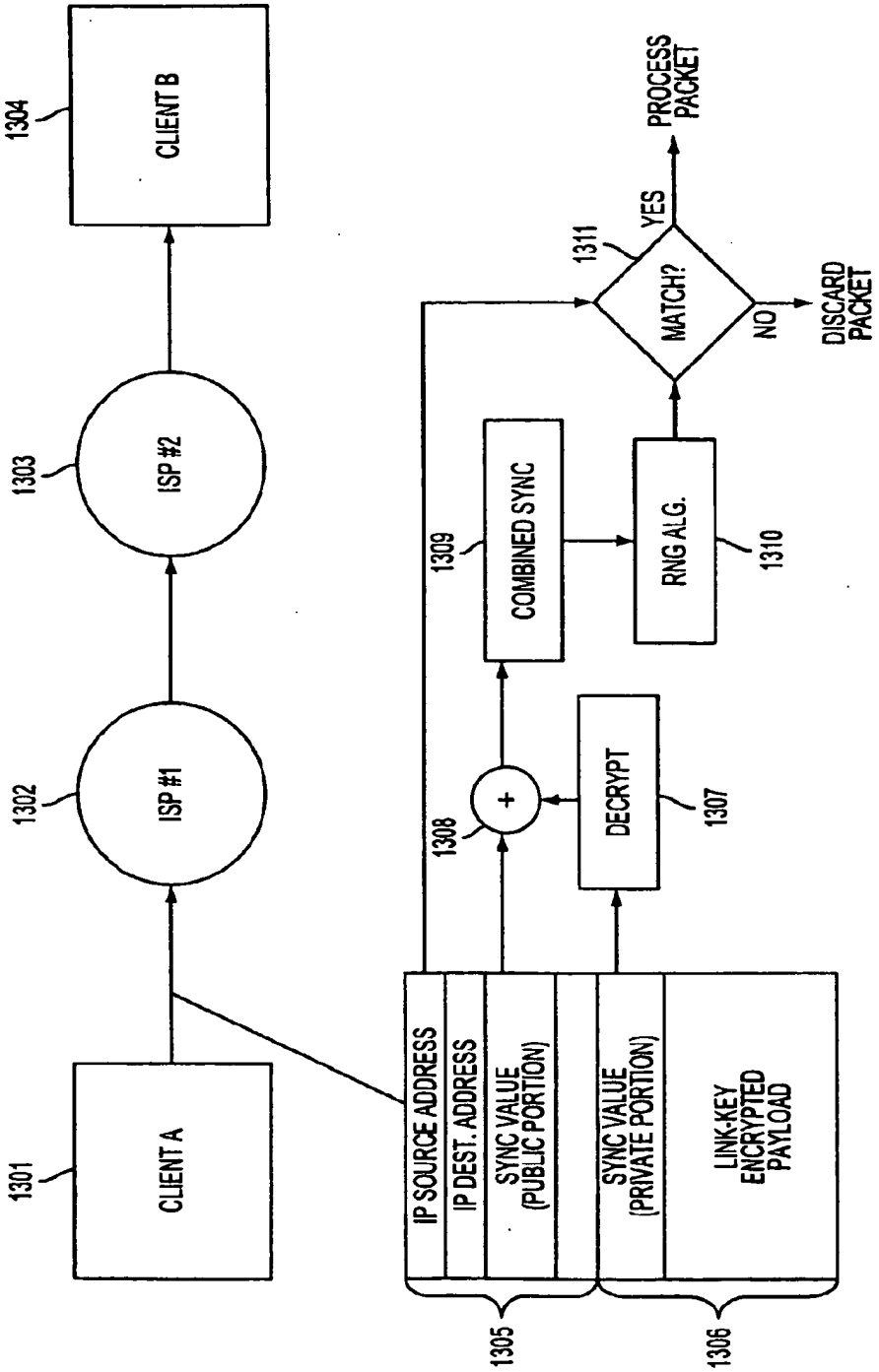

1304
CLIENT B
1303
ISP #2
1302
ISP #1
1301
CLIENT A
IP SOURCE ADDRESS
IP DEST. ADDRESS
SYNC VALUE (PUBLIC PORTION)
SYNC VALUE (PRIVATE PORTION)
LINK-KEY ENCRYPTED PAYLOAD
1305
1306
1308
+
DECRYPT
1307
1309
COMBINED SYNC
RNG ALG.
1310
1311
MATCH?
YES
PROCESS PACKET
NO
DISCARD PACKET

FIG. 13

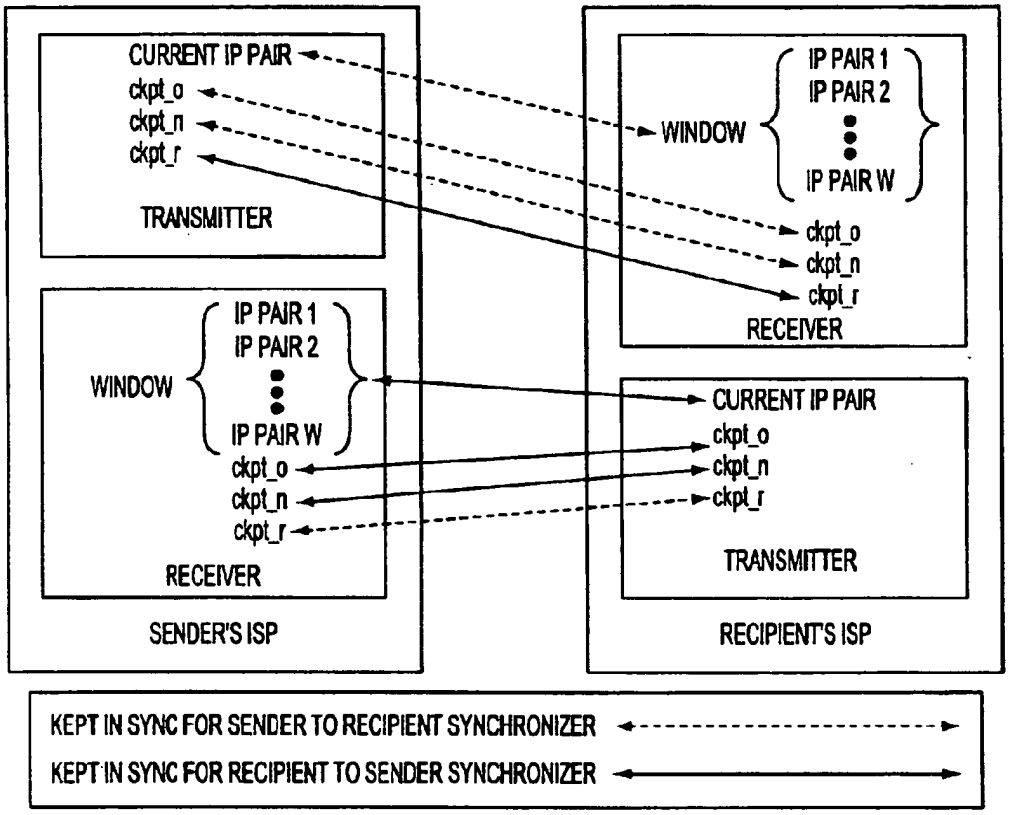

CURRENT IP PAIR
ckpt_o
ckpt_n
ckpt_r
TRANSMITTER
WINDOW
IP PAIR 1
IP PAIR 2
IP PAIR W
ckpt_o
ckpt_n
ckpt_r
RECEIVER
SENDER'S ISP
WINDOW
IP PAIR 1
IP PAIR 2
IP PAIR W
ckpt_o
ckpt_n
ckpt_r
RECEIVER
CURRENT IP PAIR
ckpt_o
ckpt_n
ckpt_r
TRANSMITTER
RECIPIENT'S ISP
KEPT IN SYNC FOR SENDER TO RECIPIENT SYNCHRONIZER
KEPT IN SYNC FOR RECIPIENT TO SENDER SYNCHRONIZER

FIG. 14

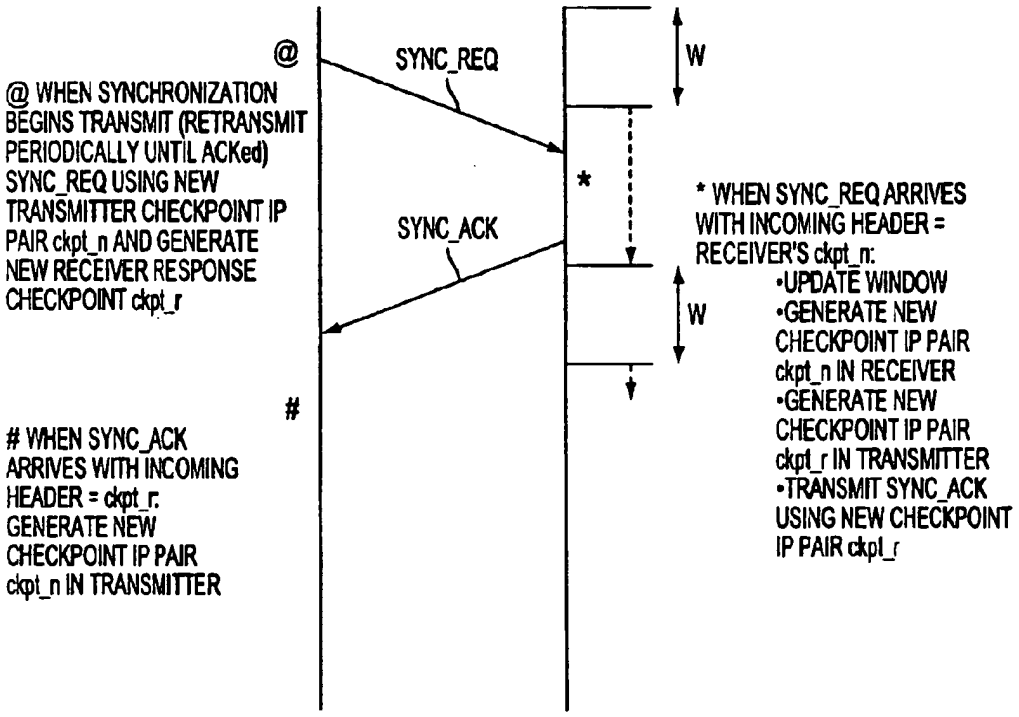

@
SYNC_REQ
W
@ WHEN SYNCHRONIZATION BEGINS TRANSMIT (RETRANSMIT PERIODICALLY UNTIL ACKed) SYNC_REQ USING NEW TRANSMITTER CHECKPOINT IP PAIR ckpt_n AND GENERATE NEW RECEIVER RESPONSE CHECKPOINT ckpt_r
*
* WHEN SYNC_REQ ARRIVES WITH INCOMING HEADER = RECEIVER'S ckpt_n:
•UPDATE WINDOW
•GENERATE NEW CHECKPOINT IP PAIR ckpt_n IN RECEIVER
•GENERATE NEW CHECKPOINT IP PAIR ckpt_r IN TRANSMITTER
•TRANSMIT SYNC_ACK USING NEW CHECKPOINT IP PAIR ckpt_r
SYNC_ACK
W
#
WHEN SYNC_ACK ARRIVES WITH INCOMING HEADER = ckpt_r:
GENERATE NEW CHECKPOINT IP PAIR ckpt_n IN TRANSMITTER

FIG. 15

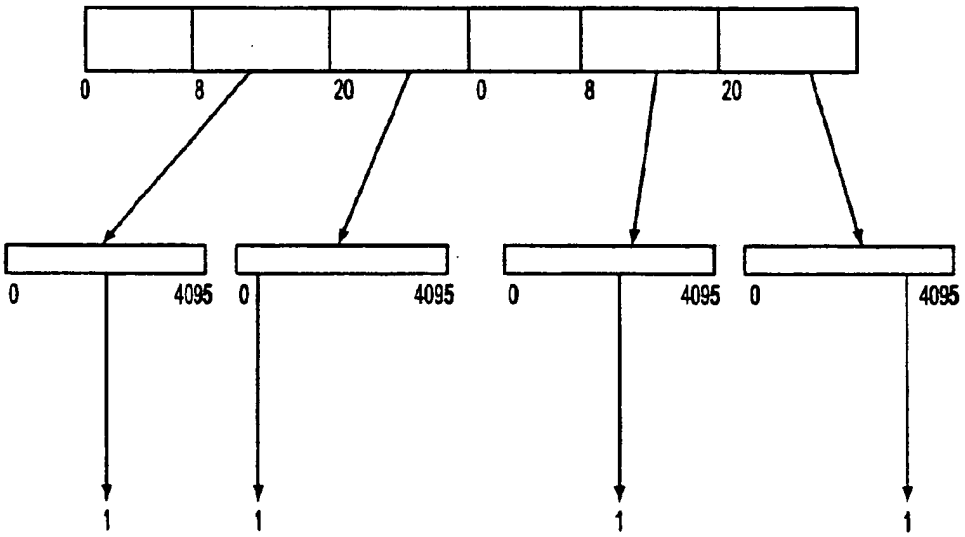


FIG. 16

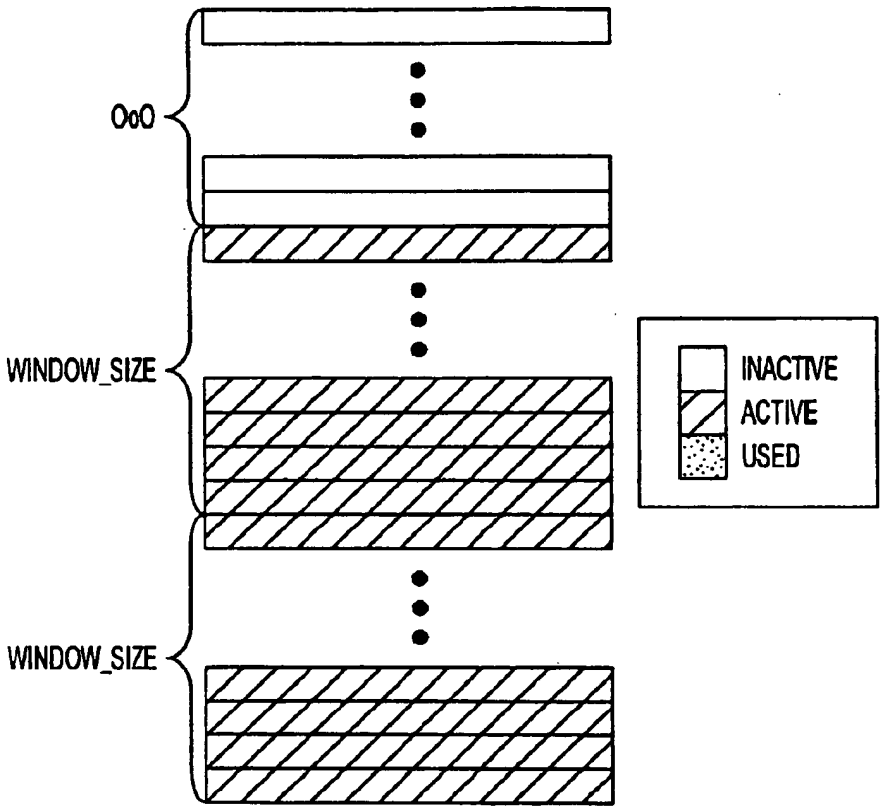


FIG. 17

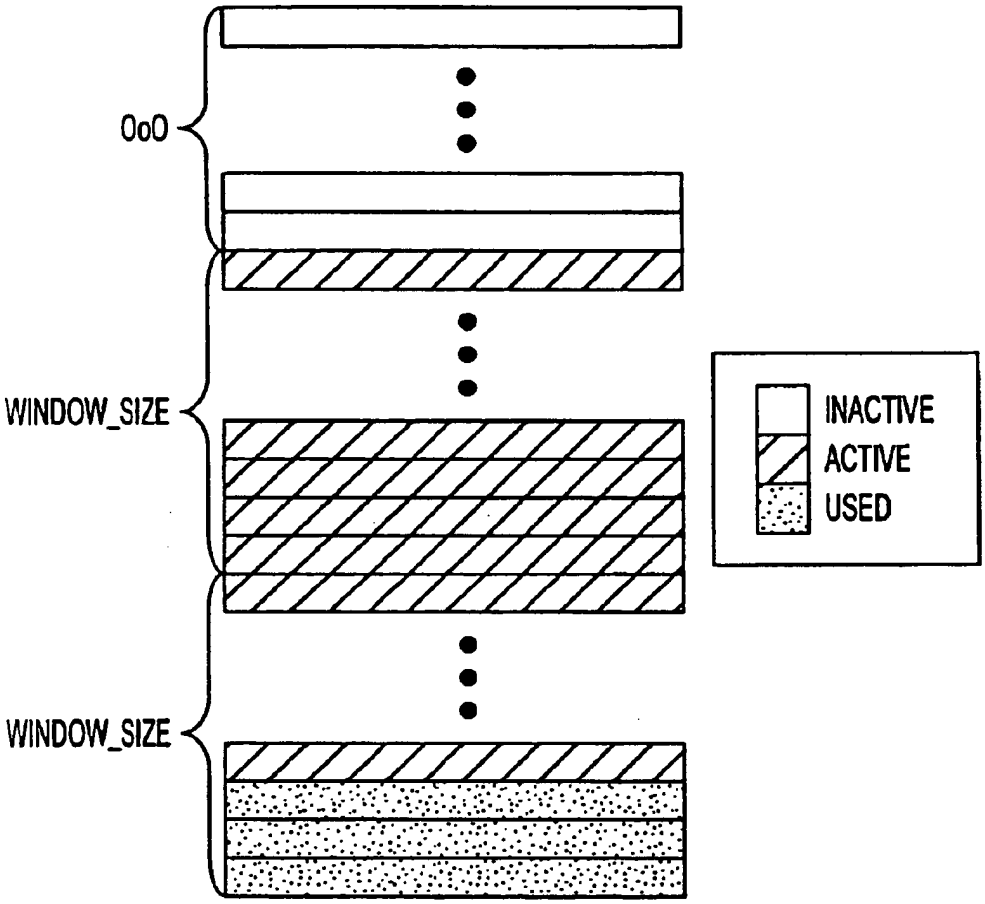


FIG. 18

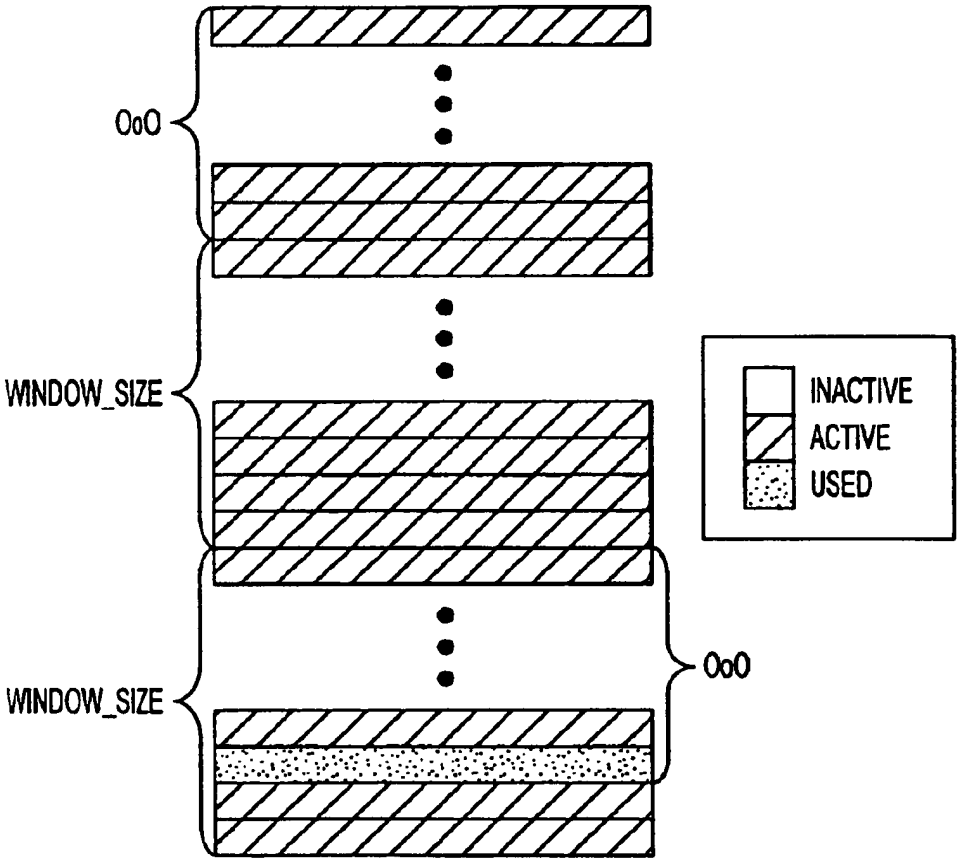


FIG. 19

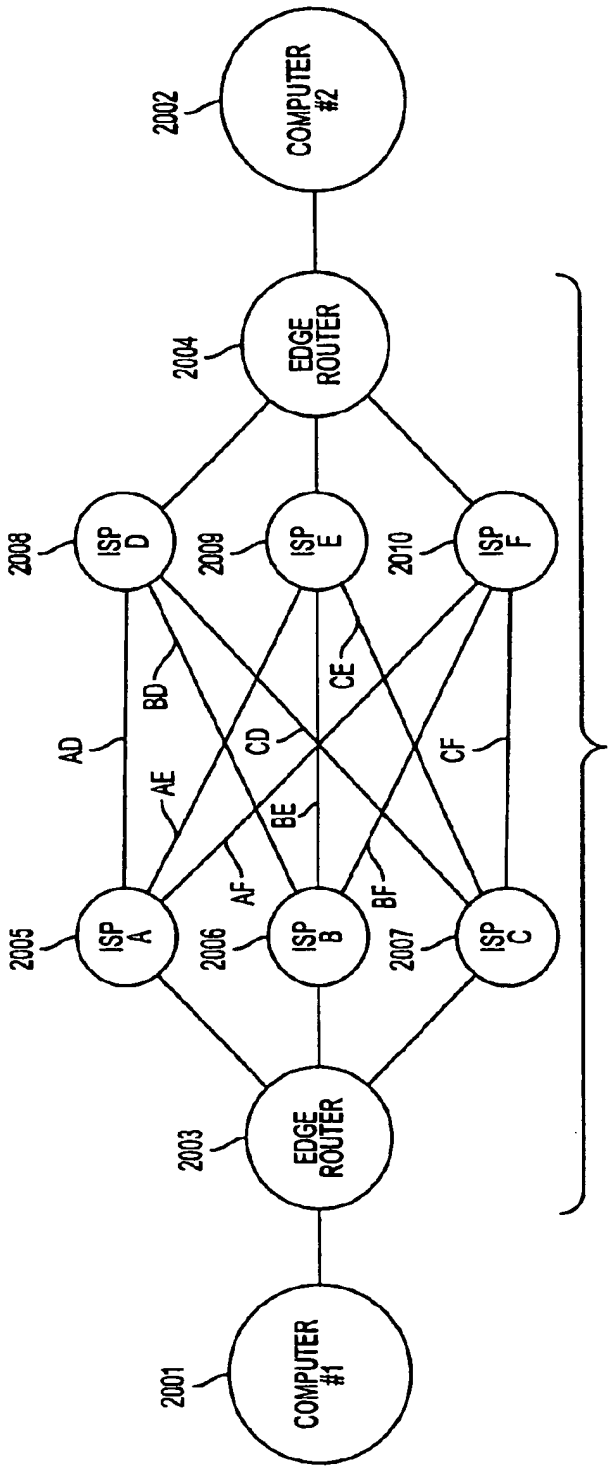

2002
COMPUTER #2
2004
EDGE ROUTER
2008
ISP D
2009
ISP E
2010
ISP F
AD
BD
CD
CE
CF
AE
BE
AF
BF
2005
ISP A
2006
ISP B
2007
ISP C
2003
EDGE ROUTER
2001
COMPUTER #1
2011

FIG. 20

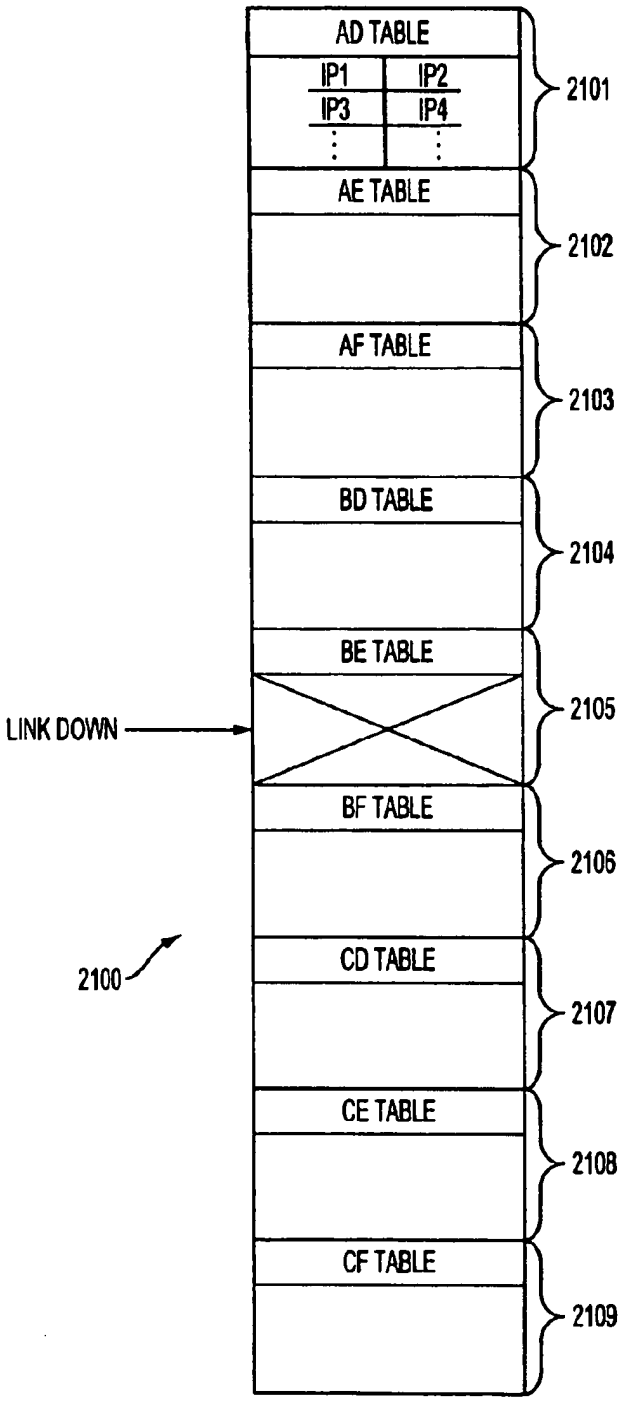

AD TABLE
IP1
IP2
IP3
IP4
2101
AE TABLE
2102
AF TABLE
2103
BD TABLE
2104
BE TABLE
2105
LINK DOWN
BF TABLE
2106
2100
CD TABLE
2107
CE TABLE
2108
CF TABLE
2109

FIG. 21

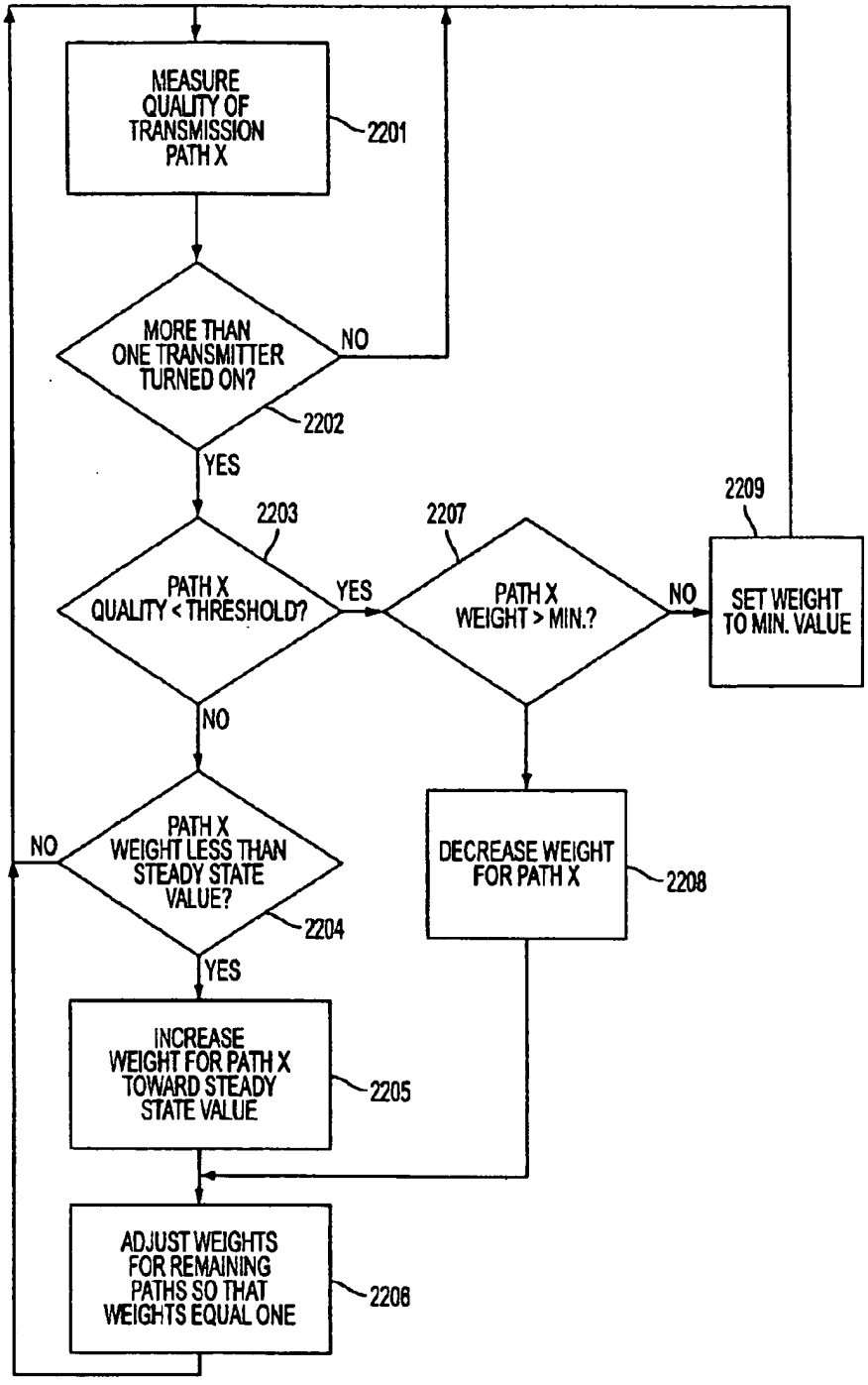

MEASURE QUALITY OF TRANSMISSION PATH X
2201
MORE THAN ONE TRANSMITTER TURNED ON?
NO
2202
YES
2203
PATH X QUALITY < THRESHOLD?
YES
2207
PATH X WEIGHT > MIN.?
NO
2209
SET WEIGHT TO MIN. VALUE
NO
PATH X WEIGHT LESS THAN STEADY STATE VALUE?
NO
2204
YES
DECREASE WEIGHT FOR PATH X
2208
INCREASE WEIGHT FOR PATH X TOWARD STEADY STATE VALUE
2205
ADJUST WEIGHTS FOR REMAINING PATHS SO THAT WEIGHTS EQUAL ONE
2206

FIG. 22A

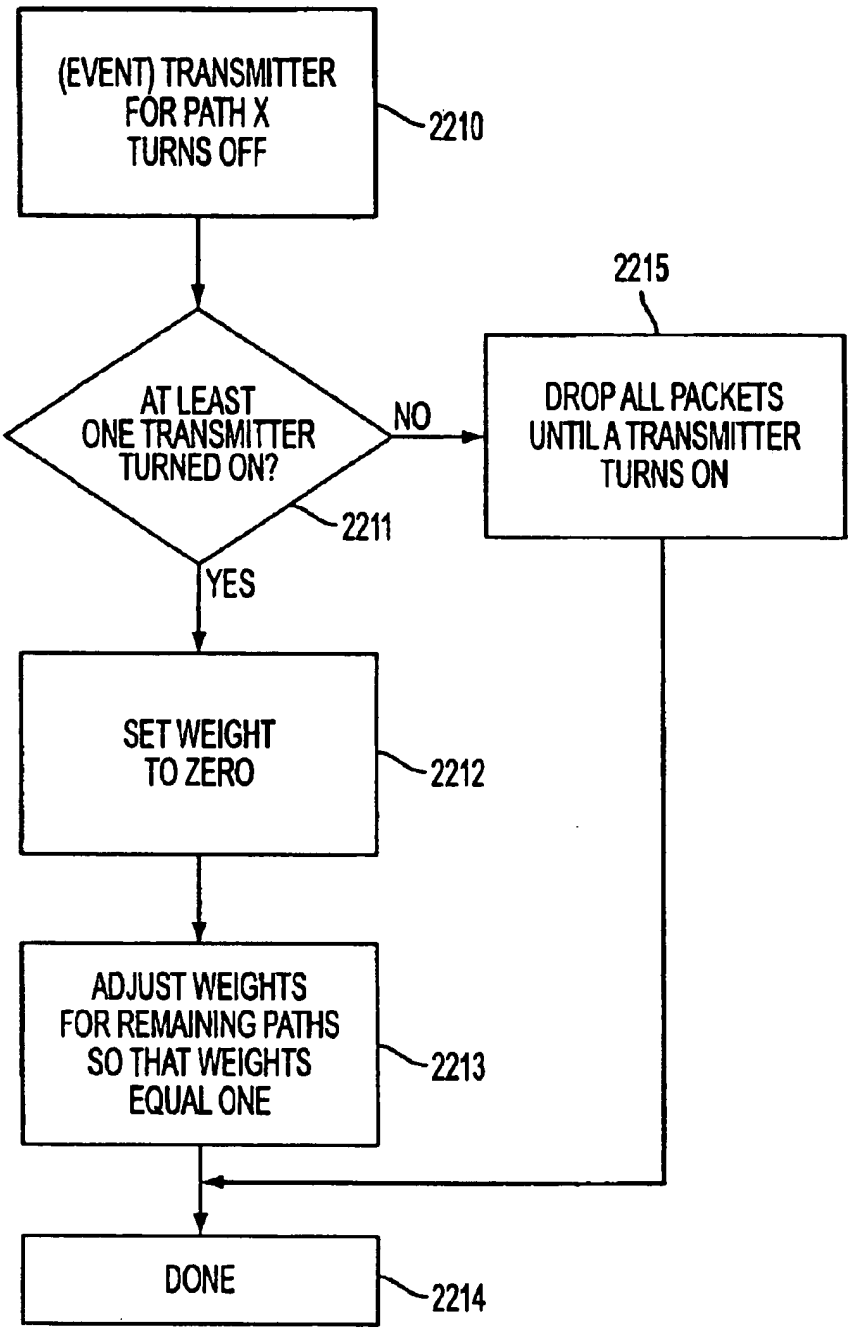

(EVENT) TRANSMITTER FOR PATH X TURNS OFF
2210
AT LEAST ONE TRANSMITTER TURNED ON?
2211
NO
2215
DROP ALL PACKETS UNTIL A TRANSMITTER TURNS ON
YES
SET WEIGHT TO ZERO
2212
ADJUST WEIGHTS FOR REMAINING PATHS SO THAT WEIGHTS EQUAL ONE
2213
DONE
2214

FIG. 22B

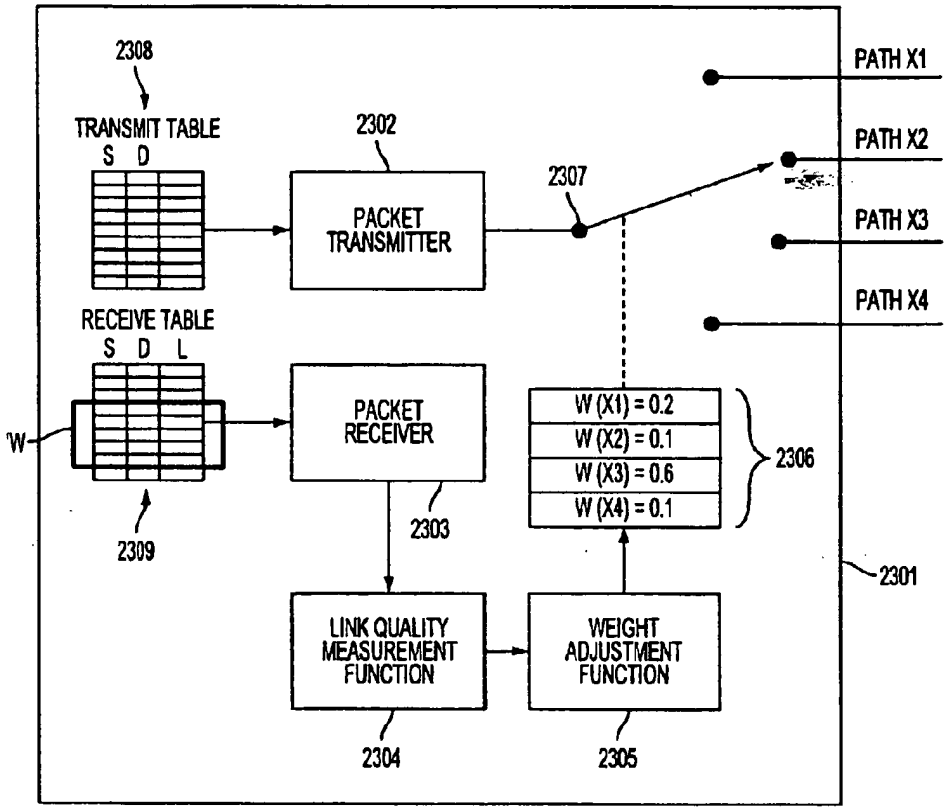

2308
TRANSMIT TABLE
S D
2302
PACKET TRANSMITTER
2307
PATH X1
PATH X2
PATH X3
PATH X4
RECEIVE TABLE
S D L
W
PACKET RECEIVER
W (X1) = 0.2
W (X2) = 0.1
W (X3) = 0.6
W (X4) = 0.1
2306
2309
2303
2301
LINK QUALITY MEASUREMENT FUNCTION
WEIGHT ADJUSTMENT FUNCTION
2304
2305

FIG. 23

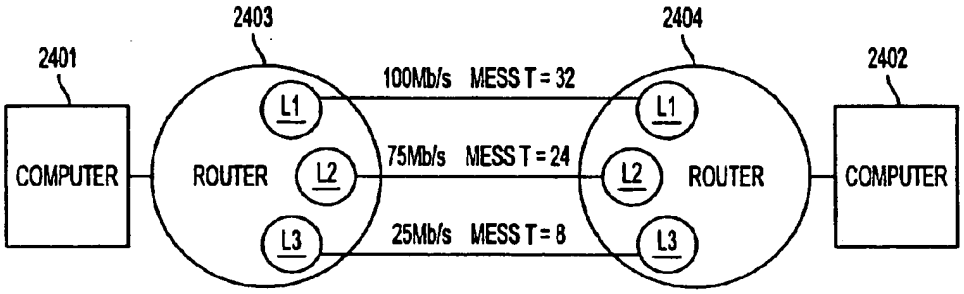

2403
2404
2401
2402
100Mb/s MESS T = 32
75Mb/s MESS T = 24
25Mb/s MESS T = 8
L1
L2
L3
L1
L2
L3
COMPUTER
ROUTER
ROUTER
COMPUTER

FIG. 24

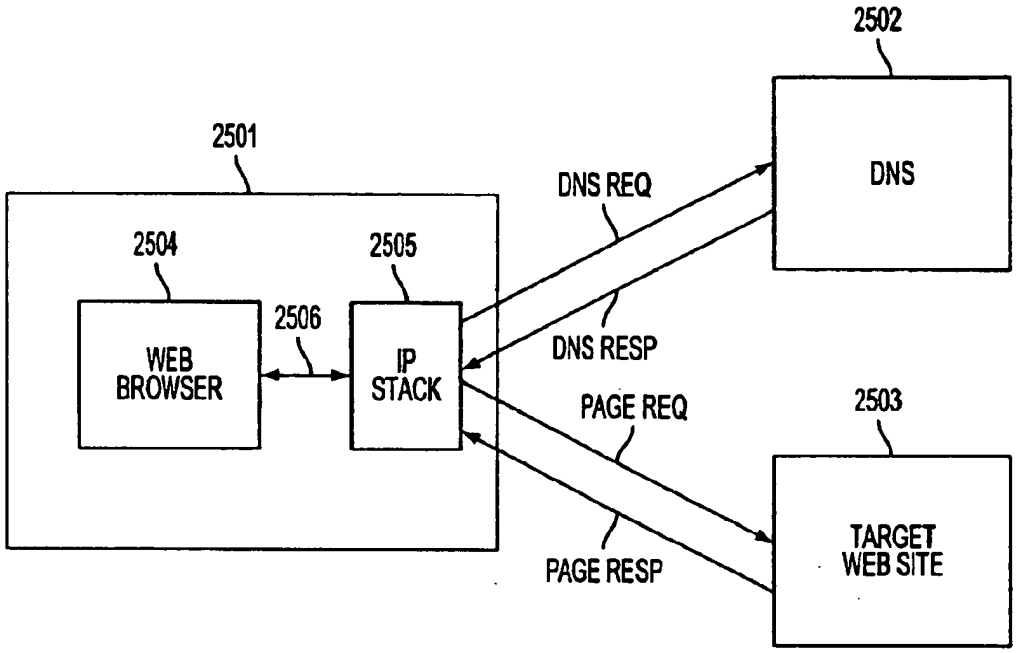


FIG. 25
(PRIOR ART)

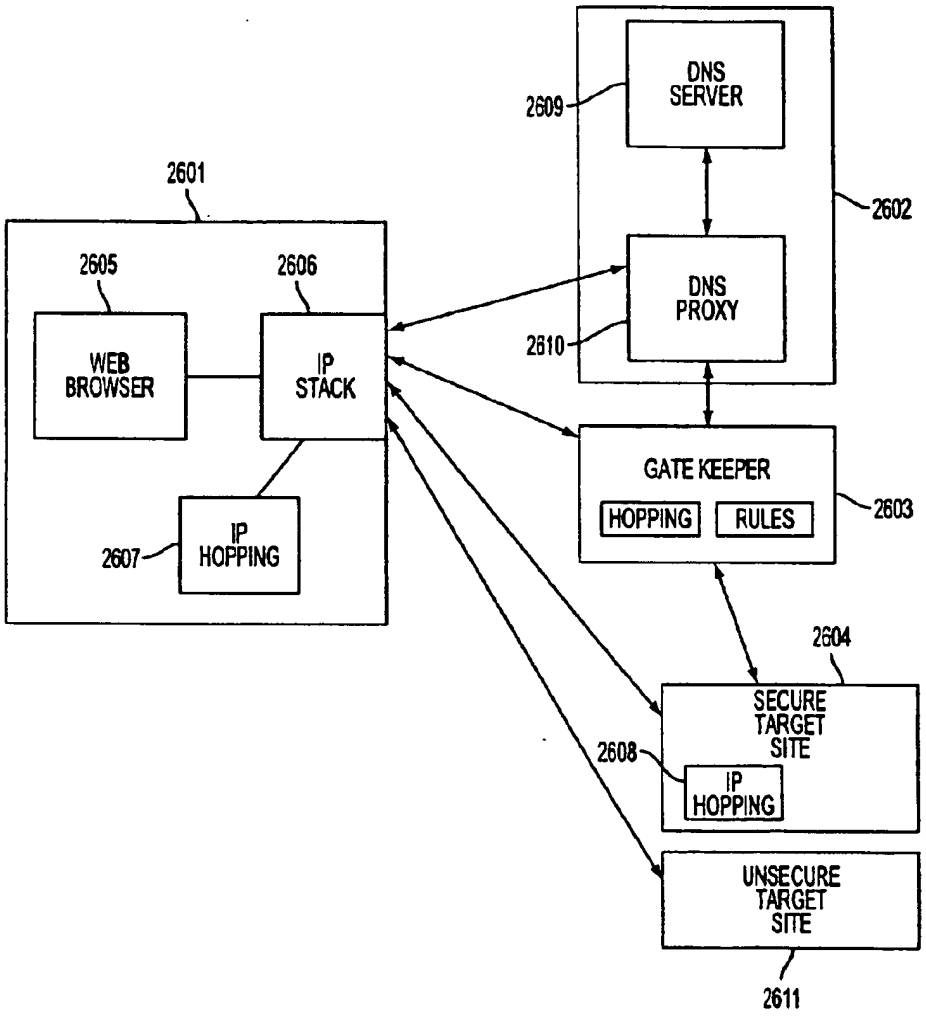

DNS SERVER
2609
2601
2602
2605
2606
DNS PROXY
WEB BROWSER
IP STACK
2610
GATE KEEPER
HOPPING
RULES
2603
IP HOPPING
2607
2604
SECURE TARGET SITE
2608
IP HOPPING
UNSECURE TARGET SITE
2611

FIG. 26

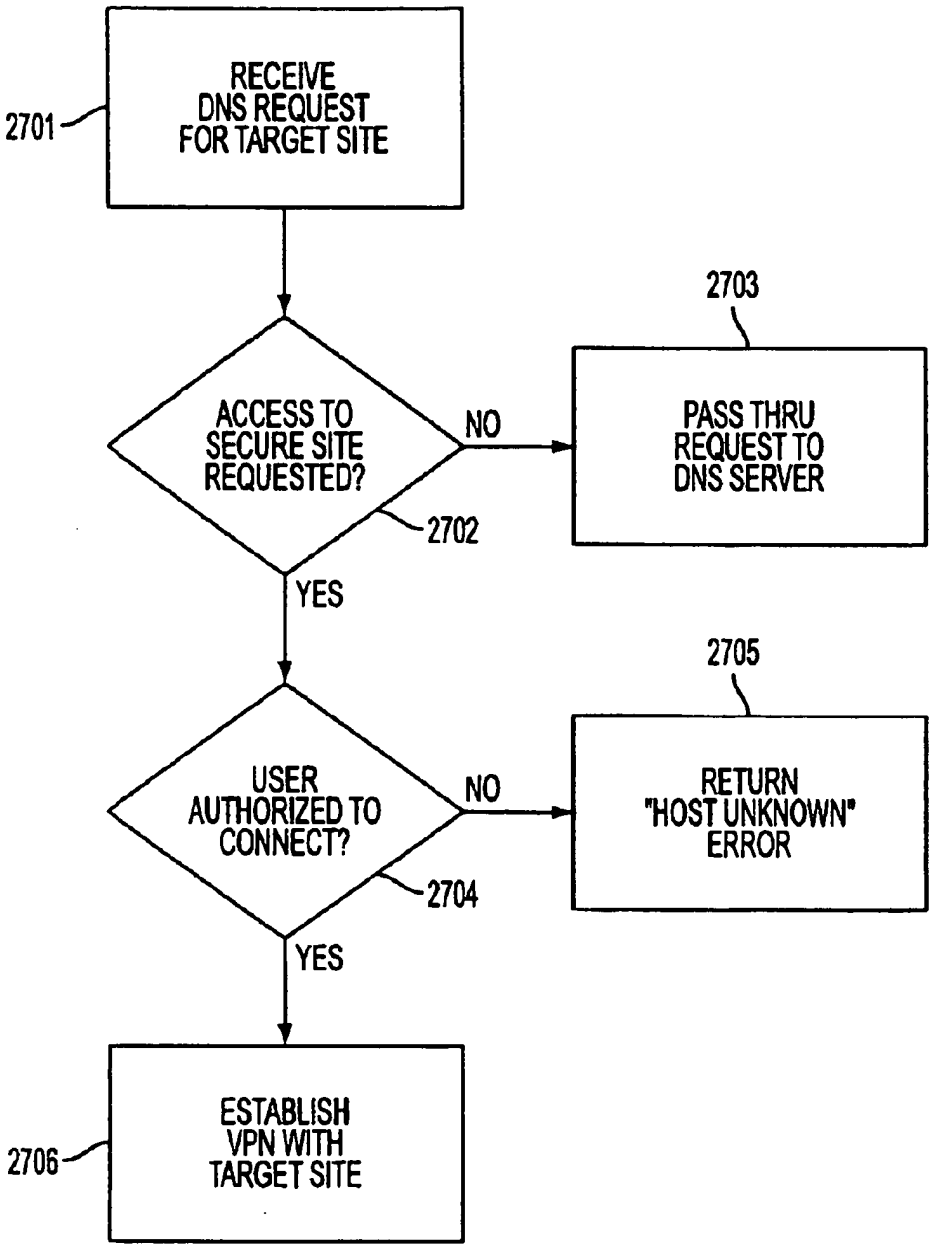

RECEIVE DNS REQUEST FOR TARGET SITE
2701
ACCESS TO SECURE SITE REQUESTED?
2702
NO
2703
PASS THRU REQUEST TO DNS SERVER
YES
USER AUTHORIZED TO CONNECT?
2704
NO
2705
RETURN "HOST UNKNOWN" ERROR
YES
ESTABLISH VPN WITH TARGET SITE
2706

FIG. 27

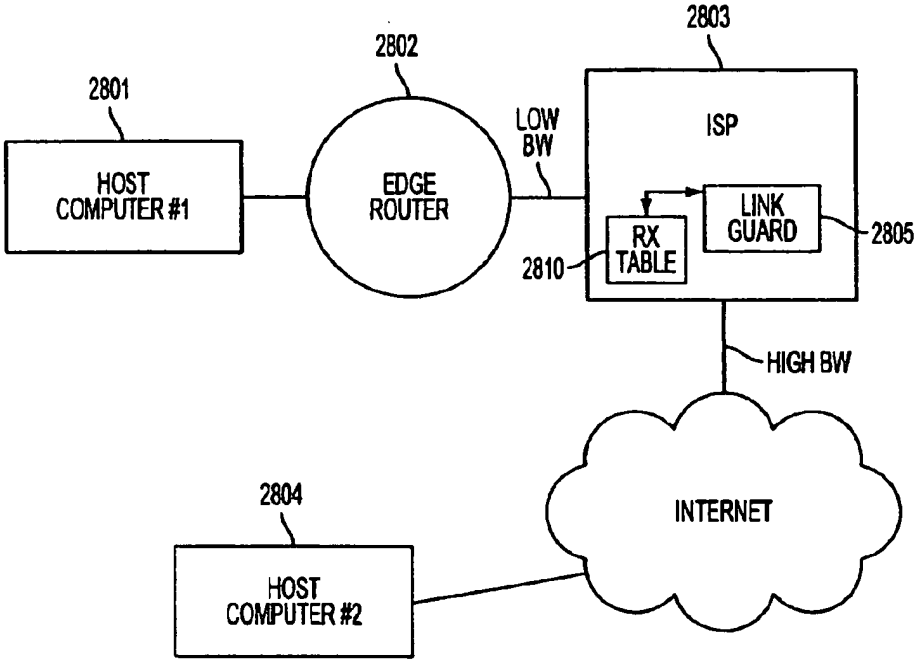

2803
2802
2801
ISP
LOW BW
HOST COMPUTER #1
EDGE ROUTER
LINK GUARD
2805
RX TABLE
2810
HIGH BW
INTERNET
2804
HOST COMPUTER #2

FIG. 28

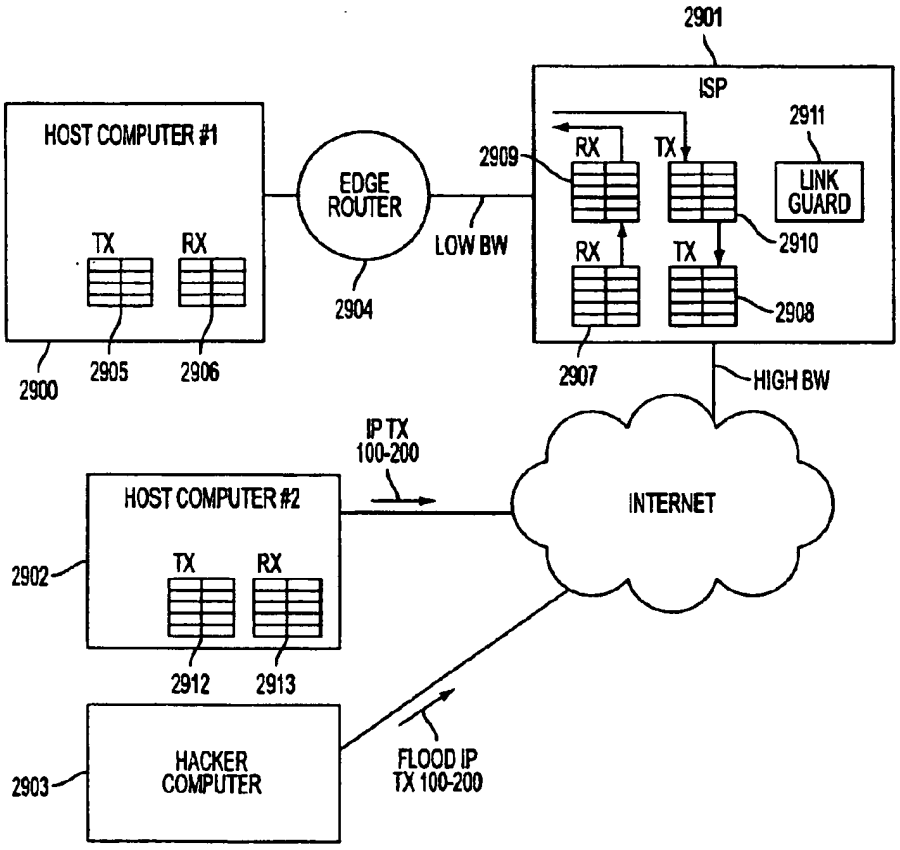

2901
ISP
2911
HOST COMPUTER #1
EDGE ROUTER
2909
RX
TX
LINK GUARD
TX
RX
LOW BW
2910
RX
TX
2904
2908
2900
2905
2906
2907
HIGH BW
IP TX 100-200
INTERNET
HOST COMPUTER #2
2902
TX
RX
2912
2913
HACKER COMPUTER
2903
FLOOD IP TX 100-200

FIG. 29

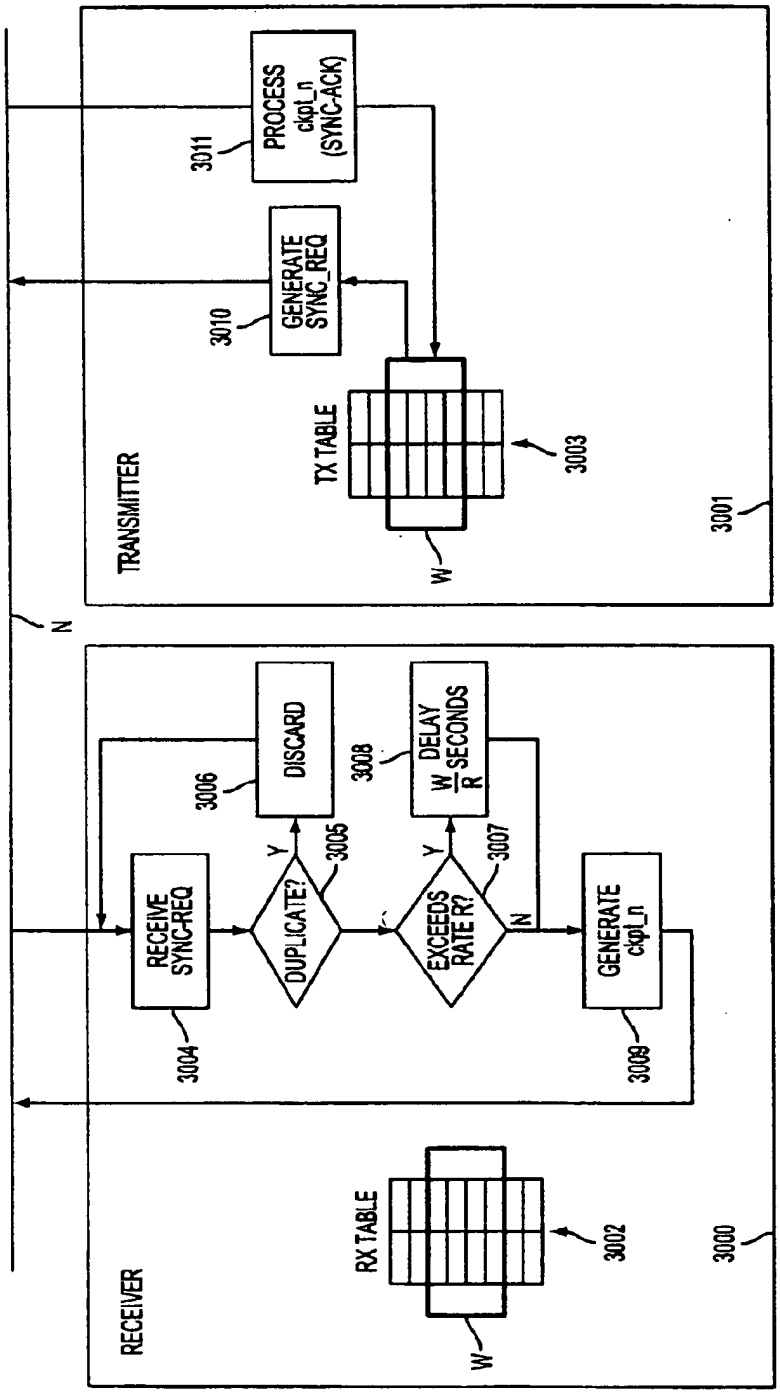

TRANSMITTER
PROCESS ckpt_n (SYNC-ACK)
3011
GENERATE SYNC_REQ
3010
TX TABLE
3003
W
3001
N
RECEIVER
RECEIVE SYNC-REQ
3004
DUPLICATE?
3005
Y
DISCARD
3006
EXCEEDS RATE R?
3007
Y
N
DELAY W/R SECONDS
3008
GENERATE ckpt_n
3009
RX TABLE
3002
W
3000

FIG. 30

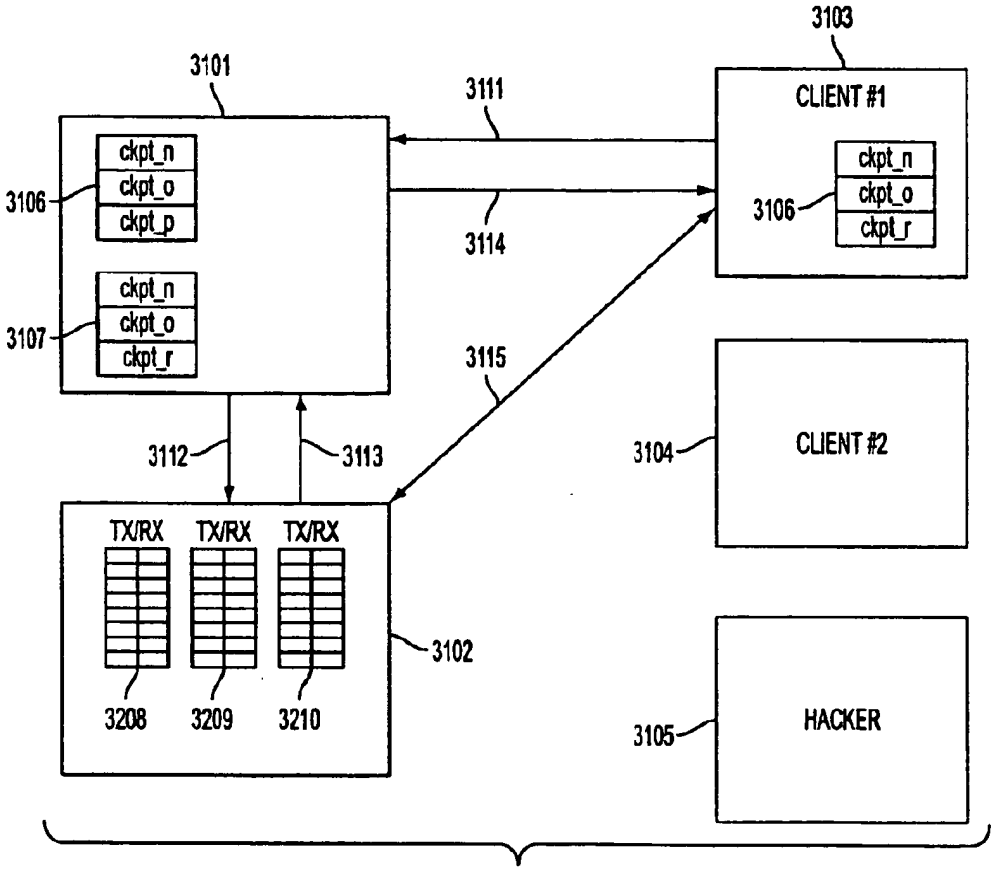

3103
3101
3111
CLIENT #1
ckpt_n
ckpt_o
ckpt_p
3106
ckpt_n
ckpt_o
ckpt_r
3106
3114
ckpt_n
ckpt_o
ckpt_r
3107
3115
3112
3113
3104
CLIENT #2
TX/RX
TX/RX
TX/RX
3102
3208
3209
3210
3105
HACKER

FIG. 31

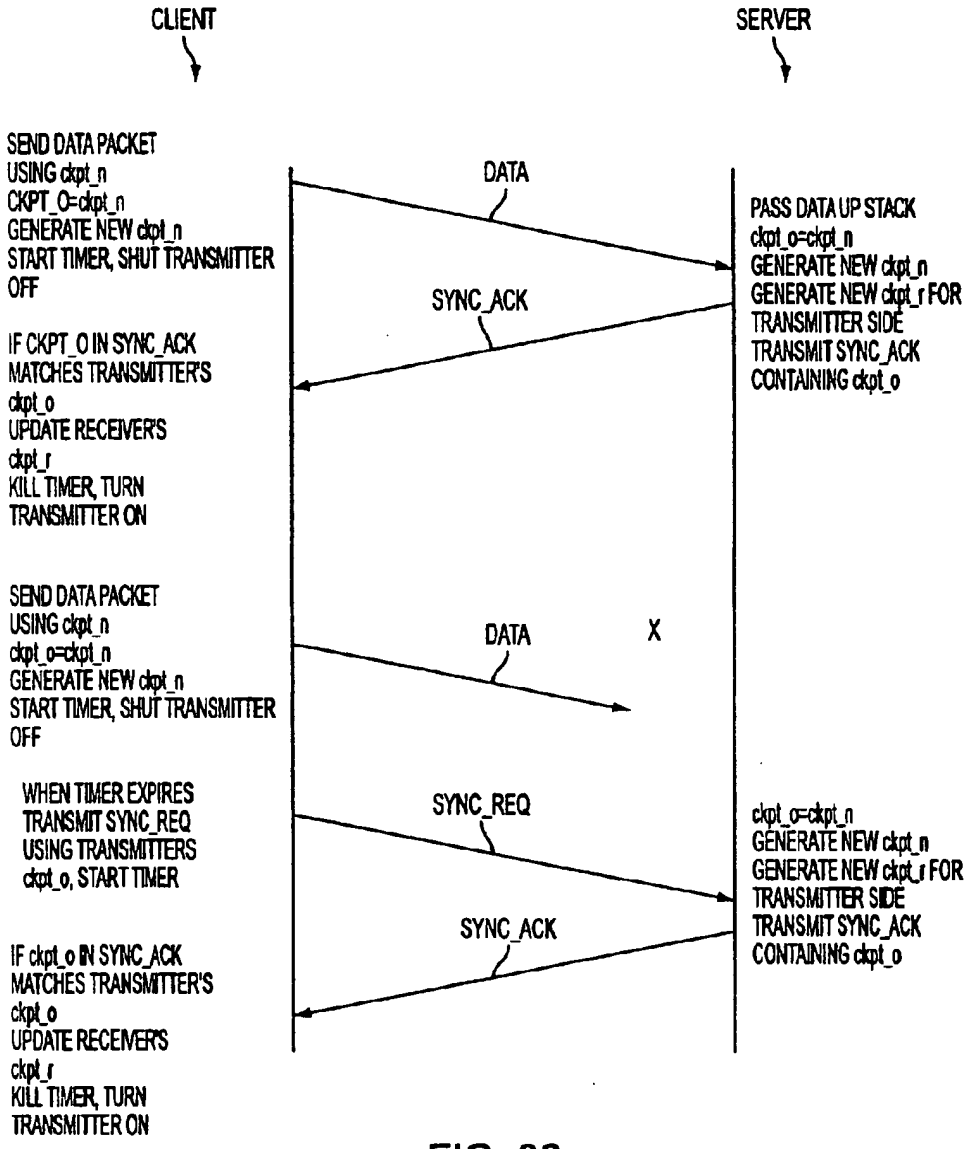

CLIENT
SERVER
SEND DATA PACKET
USING ckpt_n
CKPT_O=ckpt_n
GENERATE NEW ckpt_n
START TIMER, SHUT TRANSMITTER OFF
DATA
PASS DATA UP STACK
ckpt_o=ckpt_n
GENERATE NEW ckpt_n
GENERATE NEW ckpt_r FOR TRANSMITTER SIDE
TRANSMIT SYNC_ACK CONTAINING ckpt_o
SYNC_ACK
IF CKPT_O IN SYNC_ACK MATCHES TRANSMITTER'S ckpt_o
UPDATE RECEIVER'S ckpt_r
KILL TIMER, TURN TRANSMITTER ON
SEND DATA PACKET
USING ckpt_n
ckpt_o=ckpt_n
GENERATE NEW ckpt_n
START TIMER, SHUT TRANSMITTER OFF
DATA
X
WHEN TIMER EXPIRES
TRANSMIT SYNC_REQ
USING TRANSMITTERS ckpt_o, START TIMER
SYNC_REQ
ckpt_o=ckpt_n
GENERATE NEW ckpt_n
GENERATE NEW ckpt_r FOR TRANSMITTER SIDE
TRANSMIT SYNC_ACK CONTAINING ckpt_o
SYNC_ACK
IF ckpt_o IN SYNC_ACK MATCHES TRANSMITTER'S ckpt_o
UPDATE RECEIVER'S ckpt_r
KILL TIMER, TURN TRANSMITTER ON

FIG. 32

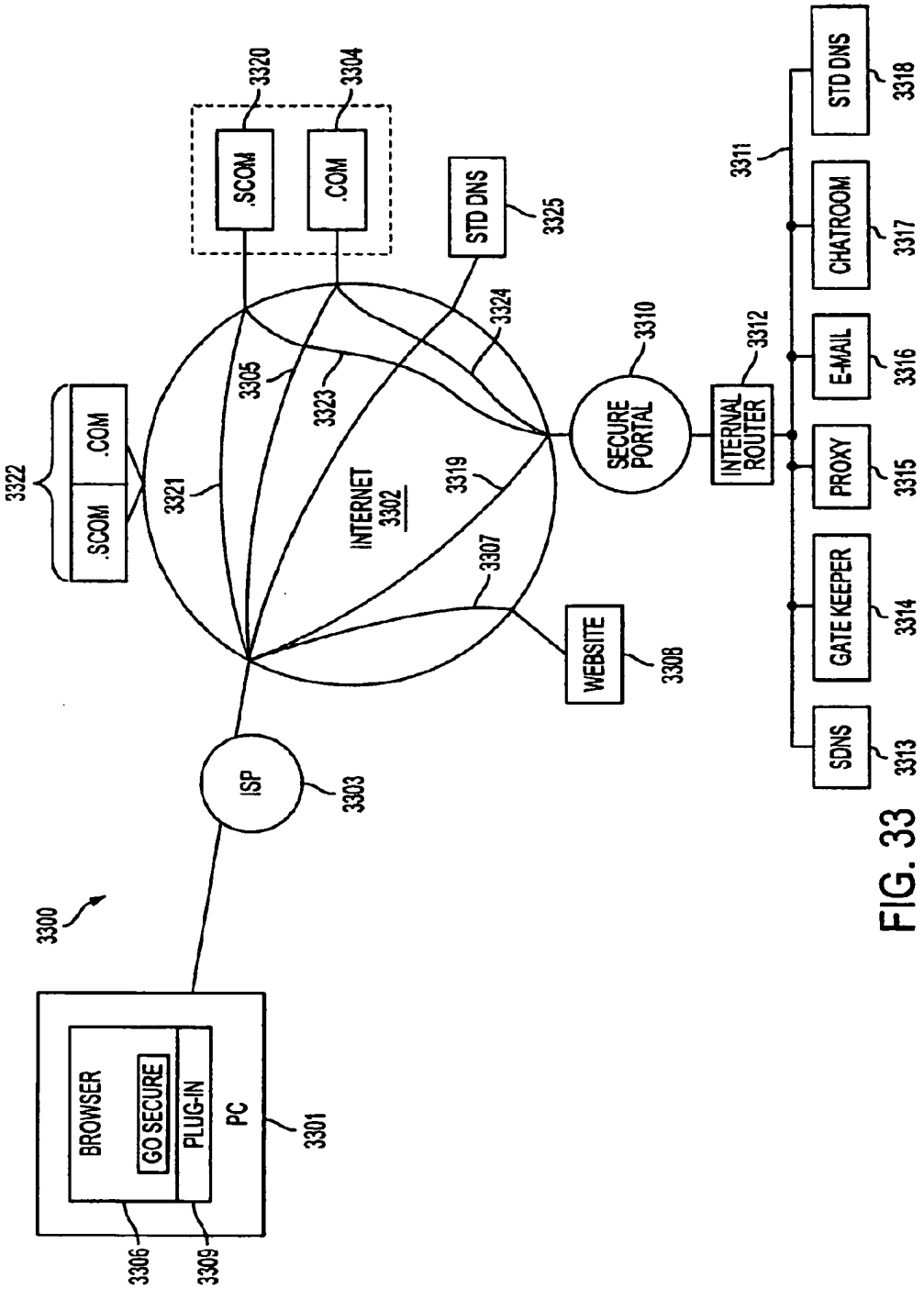

3300
PC
BROWSER
GO SECURE
PLUG-IN
3301
3306
3309
ISP
3303
INTERNET
3302
.SCOM
.COM
3322
3321
3305
3323
3324
3319
3307
3320
3304
STD DNS
3325
WEBSITE
3308
SECURE PORTAL
3310
INTERNAL ROUTER
3312
3311
STD DNS
3318
CHATROOM
3317
E-MAIL
3316
PROXY
3315
GATE KEEPER
3314
SDNS
3313

FIG. 33

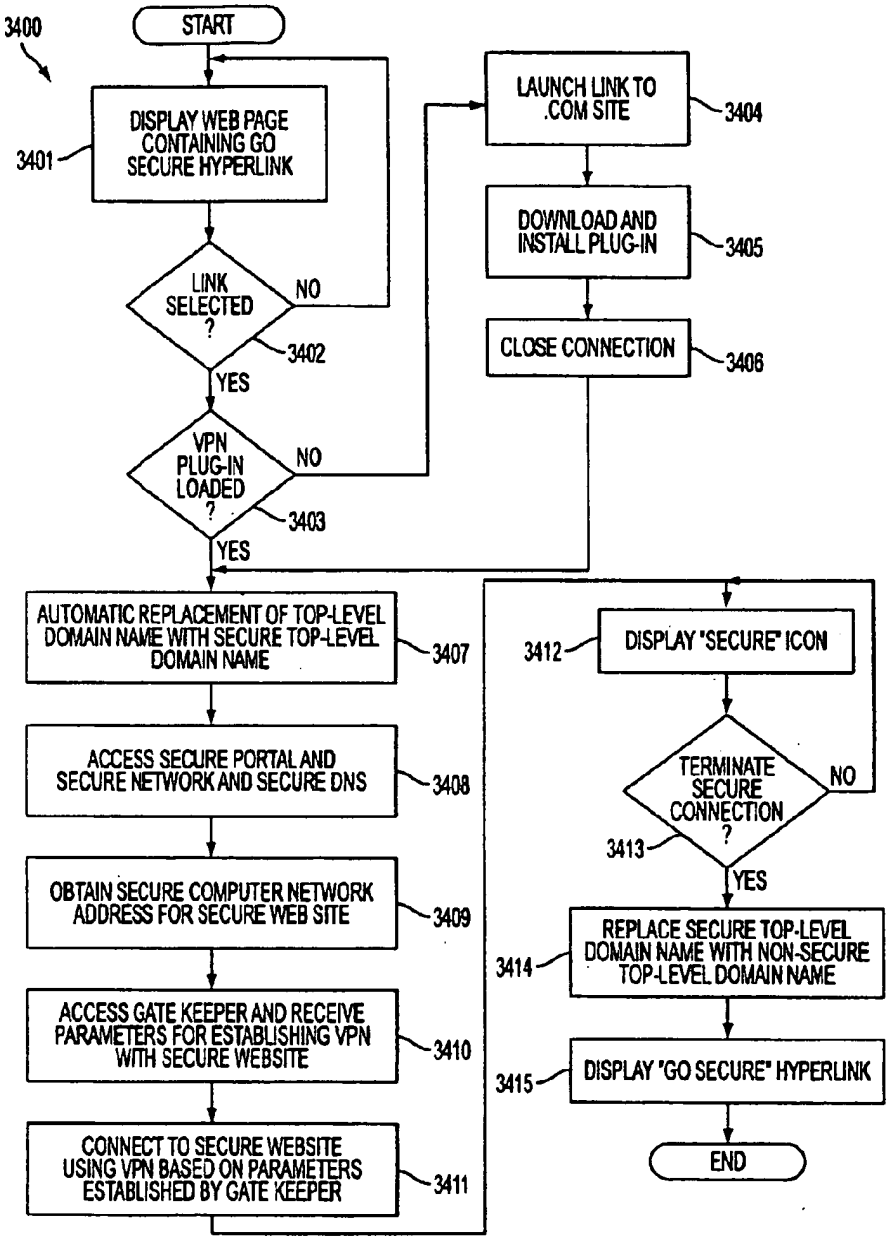

3400
START
DISPLAY WEB PAGE CONTAINING GO SECURE HYPERLINK
3401
LINK SELECTED ?
NO
3402
YES
VPN PLUG-IN LOADED ?
NO
3403
YES
LAUNCH LINK TO .COM SITE
3404
DOWNLOAD AND INSTALL PLUG-IN
3405
CLOSE CONNECTION
3406
AUTOMATIC REPLACEMENT OF TOP-LEVEL DOMAIN NAME WITH SECURE TOP-LEVEL DOMAIN NAME
3407
ACCESS SECURE PORTAL AND SECURE NETWORK AND SECURE DNS
3408
OBTAIN SECURE COMPUTER NETWORK ADDRESS FOR SECURE WEB SITE
3409
ACCESS GATE KEEPER AND RECEIVE PARAMETERS FOR ESTABLISHING VPN WITH SECURE WEBSITE
3410
CONNECT TO SECURE WEBSITE USING VPN BASED ON PARAMETERS ESTABLISHED BY GATE KEEPER
3411
3412
DISPLAY "SECURE" ICON
TERMINATE SECURE CONNECTION ?
NO
3413
YES
3414
REPLACE SECURE TOP-LEVEL DOMAIN NAME WITH NON-SECURE TOP-LEVEL DOMAIN NAME
3415
DISPLAY "GO SECURE" HYPERLINK
END

FIG. 34

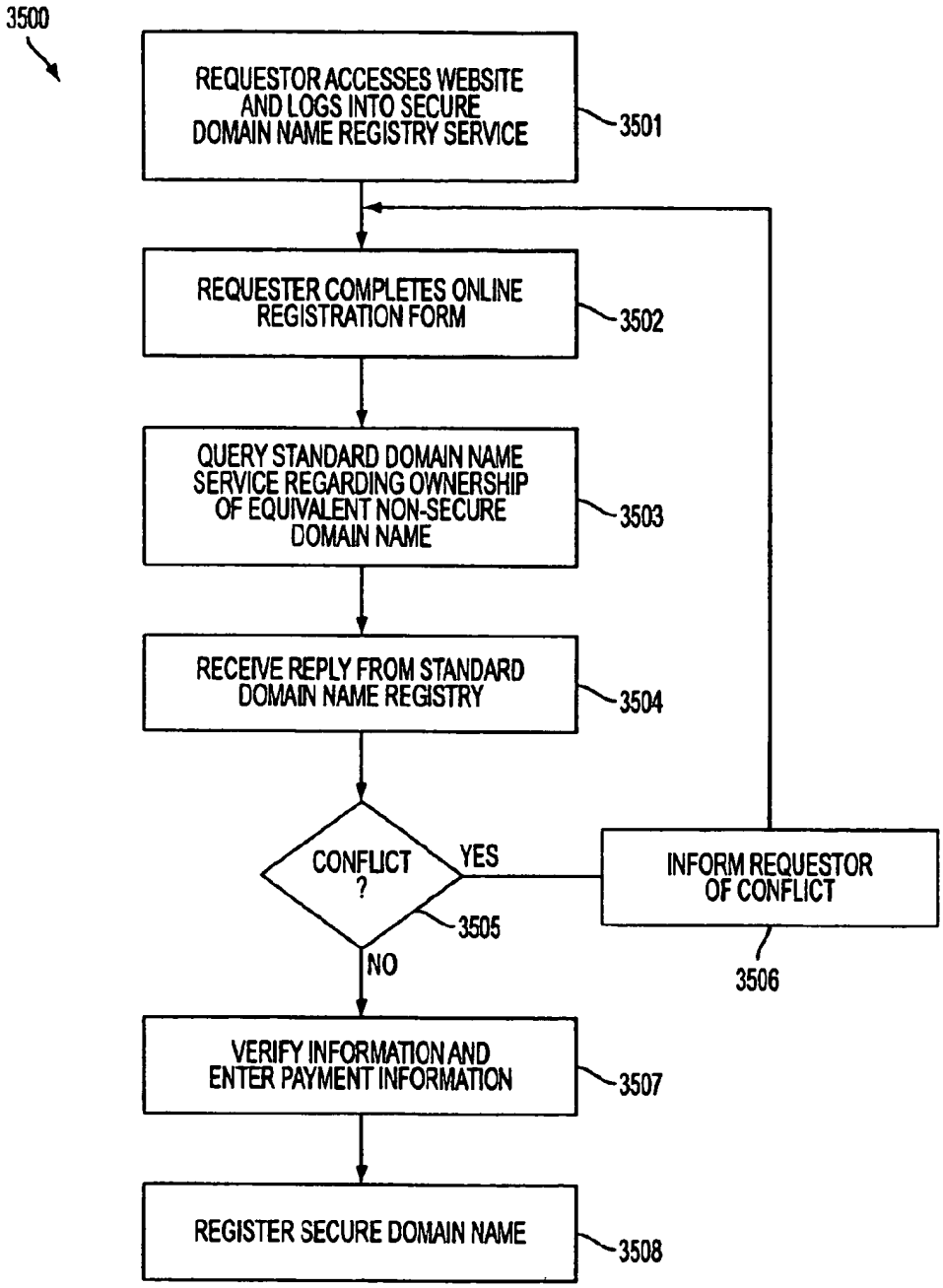

3500
REQUESTOR ACCESSES WEBSITE AND LOGS INTO SECURE DOMAIN NAME REGISTRY SERVICE
3501
REQUESTER COMPLETES ONLINE REGISTRATION FORM
3502
QUERY STANDARD DOMAIN NAME SERVICE REGARDING OWNERSHIP OF EQUIVALENT NON-SECURE DOMAIN NAME
3503
RECEIVE REPLY FROM STANDARD DOMAIN NAME REGISTRY
3504
CONFLICT ?
YES
3505
INFORM REQUESTOR OF CONFLICT
3506
NO
VERIFY INFORMATION AND ENTER PAYMENT INFORMATION
3507
REGISTER SECURE DOMAIN NAME
3508

FIG. 35

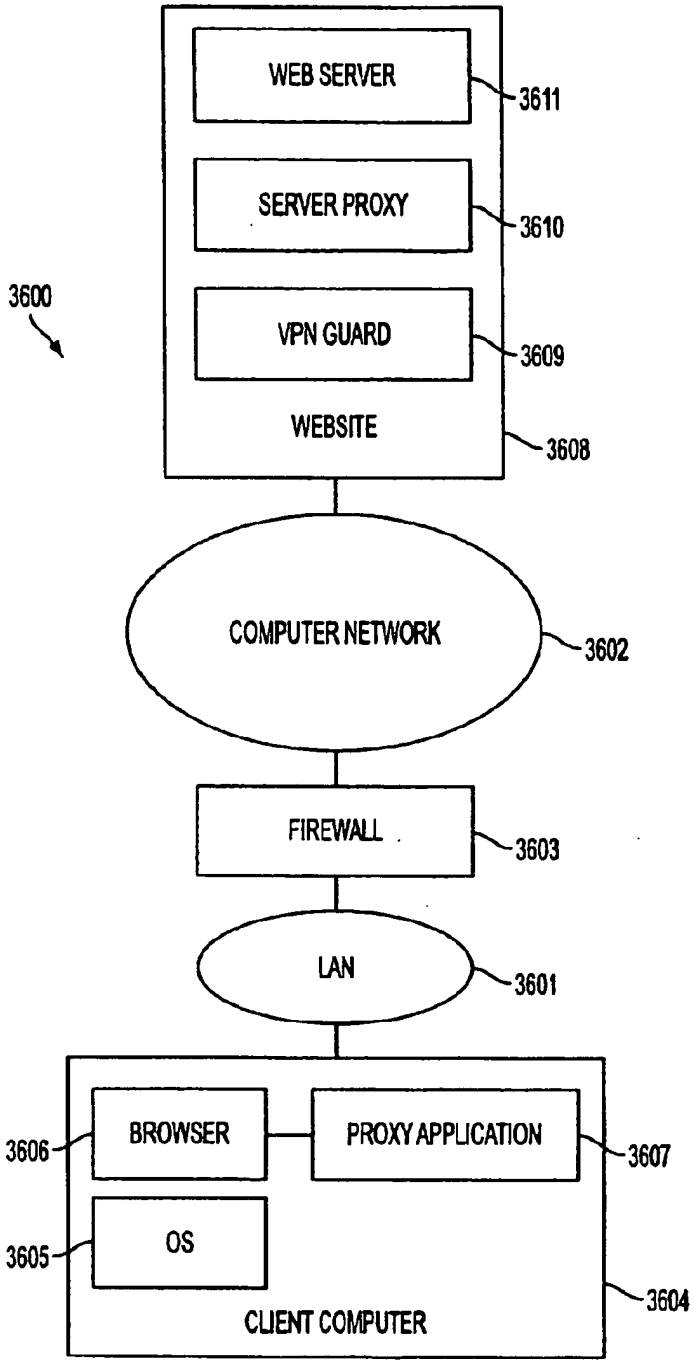

WEB SERVER
3611
SERVER PROXY
3610
3600
VPN GUARD
3609
WEBSITE
3608
COMPUTER NETWORK
3602
FIREWALL
3603
LAN
3601
BROWSER
PROXY APPLICATION
3606
3607
OS
3605
3604
CLIENT COMPUTER

FIG. 36

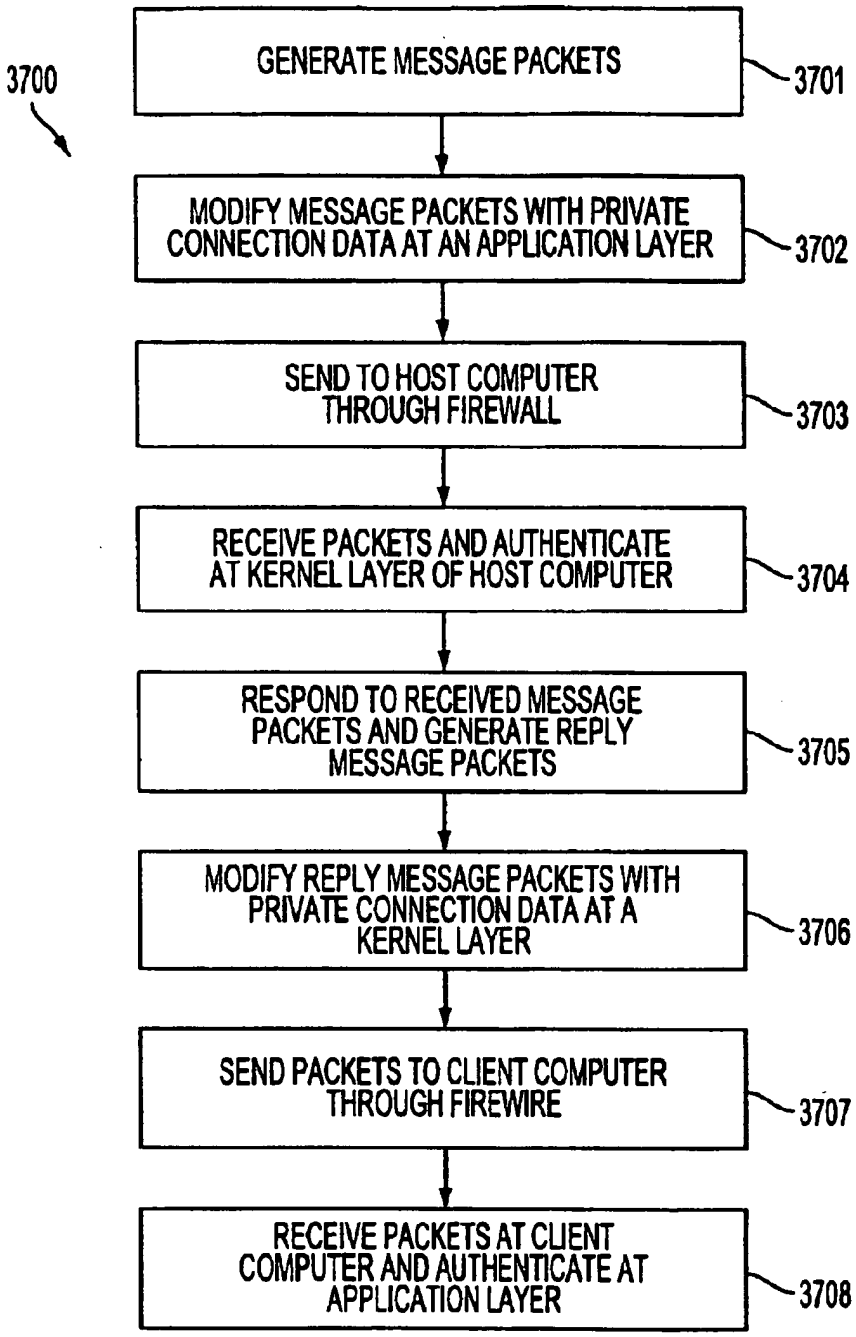

3700
GENERATE MESSAGE PACKETS
3701
MODIFY MESSAGE PACKETS WITH PRIVATE CONNECTION DATA AT AN APPLICATION LAYER
3702
SEND TO HOST COMPUTER THROUGH FIREWALL
3703
RECEIVE PACKETS AND AUTHENTICATE AT KERNEL LAYER OF HOST COMPUTER
3704
RESPOND TO RECEIVED MESSAGE PACKETS AND GENERATE REPLY MESSAGE PACKETS
3705
MODIFY REPLY MESSAGE PACKETS WITH PRIVATE CONNECTION DATA AT A KERNEL LAYER
3706
SEND PACKETS TO CLIENT COMPUTER THROUGH FIREWIRE
3707
RECEIVE PACKETS AT CLIENT COMPUTER AND AUTHENTICATE AT APPLICATION LAYER
3708

FIG. 37

METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims priority from and is a divisional patent application of U.S. application Ser. No. 09/558,209, filed Apr. 26, 2000, now abandoned which is a continuation-in-part patent application of previously-filed U.S. application Ser. No. 09/504,783, filed on Feb. 15, 2000, now U.S. Pat. No. 6,502,135, issued Dec. 31, 2002, which claims priority from and is a continuation-in-part patent application of previously-filed U.S. application Ser. No. 09/429,643, filed on Oct. 29, 1999, now U.S. Pat. No. 7,010,604, issued Mar. 7, 2006. The subject matter of U.S. application Ser. No. 09/429,643, which is bodily incorporated herein, derives from provisional U.S. application Nos. 60/106,261 (filed Oct. 30, 1998) and 60/137,704 (filed Jun. 7, 1999). The present application is also related to U.S. application Ser. No. 09/558,210, filed Apr. 26, 2000, and which is incorporated by reference herein.

BACKGROUND OF THE INVENTION

A tremendous variety of methods have been proposed and implemented to provide security and anonymity for communications over the Internet. The variety stems, in part, from the different needs of different Internet users. A basic heuristic framework to aid in discussing these different security techniques is illustrated in FIG. **1**. Two terminals, an originating terminal **100** and a destination terminal **110** are in communication over the Internet. It is desired for the communications to be secure, that is, immune to eavesdropping. For example, terminal **100** may transmit secret information to terminal **110** over the Internet **107**. Also, it may be desired to prevent an eavesdropper from discovering that terminal **100** is in communication with terminal **110**. For example, if terminal **100** is a user and terminal **110** hosts a web site, terminal **100**'s user may not want anyone in the intervening networks to know what web sites he is "visiting." Anonymity would thus be an issue, for example, for companies that want to keep their market research interests private and thus would prefer to prevent outsiders from knowing which web-sites or other Internet resources they are "visiting." These two security issues may be called data security and anonymity, respectively.

Data security is usually tackled using some form of data encryption. An encryption key **48** is known at both the originating and terminating terminals **100** and **110**. The keys may be private and public at the originating and destination terminals **100** and **110**, respectively or they may be symmetrical keys (the same key is used by both parties to encrypt and decrypt). Many encryption methods are known and usable in this context.

To hide traffic from a local administrator or ISP, a user can employ a local proxy server in communicating over an encrypted channel with an outside proxy such that the local administrator or ISP only sees the encrypted traffic. Proxy servers prevent destination servers from determining the identities of the originating clients. This system employs an intermediate server interposed between client and destination server. The destination server sees only the Internet Protocol (IP) address of the proxy server and not the originating client. The target server only sees the address of the outside proxy. This scheme relies on a trusted outside proxy server. Also, proxy schemes are vulnerable to traffic analysis methods of determining identities of transmitters and receivers. Another important limitation of proxy servers is that the server knows the identities of both calling and called parties. In many instances, an originating terminal, such as terminal A, would prefer to keep its identity concealed from the proxy, for example, if the proxy server is provided by an Internet service provider (ISP).

To defeat traffic analysis, a scheme called Chaum's mixes employs a proxy server that transmits and receives fixed length messages, including dummy messages. Multiple originating terminals are connected through a mix (a server) to multiple target servers. It is difficult to tell which of the originating terminals are communicating to which of the connected target servers, and the dummy messages confuse eavesdroppers' efforts to detect communicating pairs by analyzing traffic. A drawback is that there is a risk that the mix server could be compromised. One way to deal with this risk is to spread the trust among multiple mixes. If one mix is compromised, the identities of the originating and target terminals may remain concealed. This strategy requires a number of alternative mixes so that the intermediate servers interposed between the originating and target terminals are not determinable except by compromising more than one mix. The strategy wraps the message with multiple layers of encrypted addresses. The first mix in a sequence can decrypt only the outer layer of the message to reveal the next destination mix in sequence. The second mix can decrypt the message to reveal the next mix and so on. The target server receives the message and, optionally, a multi-layer encrypted payload containing return information to send data back in the same fashion. The only way to defeat such a mix scheme is to collude among mixes. If the packets are all fixed-length and intermixed with dummy packets, there is no way to do any kind of traffic analysis.

Still another anonymity technique, called 'crowds,' protects the identity of the originating terminal from the intermediate proxies by providing that originating terminals belong to groups of proxies called crowds. The crowd proxies are interposed between originating and target terminals. Each proxy through which the message is sent is randomly chosen by an upstream proxy. Each intermediate proxy can send the message either to another randomly chosen proxy in the "crowd" or to the destination. Thus, even crowd members cannot determine if a preceding proxy is the originator of the message or if it was simply passed from another proxy.

ZKS (Zero-Knowledge Systems) Anonymous IP Protocol allows users to select up to any of five different pseudonyms, while desktop software encrypts outgoing traffic and wraps it in User Datagram Protocol (UDP) packets. The first server in a 2+-hop system gets the UDP packets, strips off one layer of encryption to add another, then sends the traffic to the next server, which strips off yet another layer of encryption and adds a new one. The user is permitted to control the number of hops. At the final server, traffic is decrypted with an untraceable IP address. The technique is called onion-routing. This method can be defeated using traffic analysis. For a simple example, bursts of packets from a user during low-duty periods can reveal the identities of sender and receiver.

Firewalls attempt to protect LANs from unauthorized access and hostile exploitation or damage to computers connected to the LAN. Firewalls provide a server through which all access to the LAN must pass. Firewalls are centralized systems that require administrative overhead to

maintain. They can be compromised by virtual-machine applications ("applets"). They instill a false sense of security that leads to security breaches for example by users sending sensitive information to servers outside the firewall or encouraging use of modems to sidestep the firewall security. Firewalls are not useful for distributed systems such as business travelers, extranets, small teams, etc.

SUMMARY OF THE INVENTION

A secure mechanism for communicating over the internet, including a protocol referred to as the Tunneled Agile Routing Protocol (TARP), uses a unique two-layer encryption format and special TARP routers. TARP routers are similar in function to regular IP routers. Each TARP router has one or more IP addresses and uses normal IP protocol to send IP packet messages ("packets" or "datagrams"). The IP packets exchanged between TARP terminals via TARP routers are actually encrypted packets whose true destination address is concealed except to TARP routers and servers. The normal or "clear" or "outside" IP header attached to TARP IP packets contains only the address of a next hop router or destination server. That is, instead of indicating a final destination in the destination field of the IP header, the TARP packet's IP header always points to a next-hop in a series of TARP router hops, or to the final destination. This means there is no overt indication from an intercepted TARP packet of the true destination of the TARP packet since the destination could always be next-hop TARP router as well as the final destination.

Each TARP packet's true destination is concealed behind a layer of encryption generated using a link key. The link key is the encryption key used for encrypted communication between the hops intervening between an originating TARP terminal and a destination TARP terminal. Each TARP router can remove the outer layer of encryption to reveal the destination router for each TARP packet. To identify the link key needed to decrypt the outer layer of encryption of a TARP packet, a receiving TARP or routing terminal may identify the transmitting terminal by the sender/receiver IP numbers in the cleartext IP header.

Once the outer layer of encryption is removed, the TARP router determines the final destination. Each TARP packet **140** undergoes a minimum number of hops to help foil traffic analysis. The hops may be chosen at random or by a fixed value. As a result, each TARP packet may make random trips among a number of geographically disparate routers before reaching its destination. Each trip is highly likely to be different for each packet composing a given message because each trip is independently randomly determined. This feature is called agile routing. The fact that different packets take different routes provides distinct advantages by making it difficult for an interloper to obtain all the packets forming an entire multi-packet message. The associated advantages have to do with the inner layer of encryption discussed below. Agile routing is combined with another feature that furthers this purpose; a feature that ensures that any message is broken into multiple packets.

The IP address of a TARP router can be changed, a feature called IP agility. Each TARP router, independently or under direction from another TARP terminal or router, can change its IP address. A separate, unchangeable identifier or address is also defined. This address, called the TARP address, is known only to TARP routers and terminals and may be correlated at any time by a TARP router or a TARP terminal using a Lookup Table (LUT). When a TARP router or terminal changes its IP address, it updates the other TARP routers and terminals which in turn update their respective LUTs.

The message payload is hidden behind an inner layer of encryption in the TARP packet that can only be unlocked using a session key. The session key is not available to any of the intervening TARP routers. The session key is used to decrypt the payloads of the TARP packets permitting the data stream to be reconstructed.

Communication may be made private using link and session keys, which in turn may be shared and used according to any desired method. For example, public/private keys or symmetric keys may be used.

To transmit a data stream, a TARP originating terminal constructs a series of TARP packets from a series of IP packets generated by a network (IP) layer process. (Note that the terms "network layer," "data link layer," "application layer," etc. used in this specification correspond to the Open Systems Interconnection (OSI) network terminology.) The payloads of these packets are assembled into a block and chain-block encrypted using the session key. This assumes, of course, that all the IP packets are destined for the same TARP terminal. The block is then interleaved and the interleaved encrypted block is broken into a series of payloads, one for each TARP packet to be generated. Special TARP headers IPT are then added to each payload using the IP headers from the data stream packets. The TARP headers can be identical to normal IP headers or customized in some way. They should contain a formula or data for deinterleaving the data at the destination TARP terminal, a time-to-live (TTL) parameter to indicate the number of hops still to be executed, a data type identifier which indicates whether the payload contains, for example, TCP or UDP data, the sender's TARP address, the destination TARP address, and an indicator as to whether the packet contains real or decoy data or a formula for filtering out decoy data if decoy data is spread in some way through the TARP payload data.

Note that although chain-block encryption is discussed here with reference to the session key, any encryption method may be used. Preferably, as in chain block encryption, a method should be used that makes unauthorized decryption difficult without an entire result of the encryption process. Thus, by separating the encrypted block among multiple packets and making it difficult for an interloper to obtain access to all of such packets, the contents of the communications are provided an extra layer of security.

Decoy or dummy data can be added to a stream to help foil traffic analysis by reducing the peak-to-average network load. It may be desirable to provide the TARP process with an ability to respond to the time of day or other criteria to generate more decoy data during low traffic periods so that communication bursts at one point in the Internet cannot be tied to communication bursts at another point to reveal the communicating endpoints.

Dummy data also helps to break the data into a larger number of inconspicuously-sized packets permitting the interleave window size to be increased while maintaining a reasonable size for each packet. (The packet size can be a single standard size or selected from a fixed range of sizes.) One primary reason for desiring for each message to be broken into multiple packets is apparent if a chain block encryption scheme is used to form the first encryption layer prior to interleaving. A single block encryption may be applied to portion, or entirety, of a message, and that portion or entirety then interleaved into a number of separate packets. Considering the agile IP routing of the packets, and the attendant difficulty of reconstructing an entire sequence

of packets to form a single block-encrypted message element, decoy packets can significantly increase the difficulty of reconstructing an entire data stream.

The above scheme may be implemented entirely by processes operating between the data link layer and the network layer of each server or terminal participating in the TARP system. Because the encryption system described above is insertable between the data link and network layers, the processes involved in supporting the encrypted communication may be completely transparent to processes at the IP (network) layer and above. The TARP processes may also be completely transparent to the data link layer processes as well. Thus, no operations at or above the Network layer, or at or below the data link layer, are affected by the insertion of the TARP stack. This provides additional security to all processes at or above the network layer, since the difficulty of unauthorized penetration of the network layer (by, for example, a hacker) is increased substantially. Even newly developed servers running at the session layer leave all processes below the session layer vulnerable to attack. Note that in this architecture, security is distributed. That is, notebook computers used by executives on the road, for example, can communicate over the Internet without any compromise in security.

IP address changes made by TARP terminals and routers can be done at regular intervals, at random intervals, or upon detection of "attacks." The variation of IP addresses hinders traffic analysis that might reveal which computers are communicating, and also provides a degree of immunity from attack. The level of immunity from attack is roughly proportional to the rate at which the IP address of the host is changing.

As mentioned, IP addresses may be changed in response to attacks. An attack may be revealed, for example, by a regular series of messages indicating that a router is being probed in some way. Upon detection of an attack, the TARP layer process may respond to this event by changing its IP address. In addition, it may create a subprocess that maintains the original IP address and continues interacting with the attacker in some manner.

Decoy packets may be generated by each TARP terminal on some basis determined by an algorithm. For example, the algorithm may be a random one which calls for the generation of a packet on a random basis when the terminal is idle. Alternatively, the algorithm may be responsive to time of day or detection of low traffic to generate more decoy packets during low traffic times. Note that packets are preferably generated in groups, rather than one by one, the groups being sized to simulate real messages. In addition, so that decoy packets may be inserted in normal TARP message streams, the background loop may have a latch that makes it more likely to insert decoy packets when a message stream is being received. Alternatively, if a large number of decoy packets is received along with regular TARP packets, the algorithm may increase the rate of dropping of decoy packets rather than forwarding them. The result of dropping and generating decoy packets in this way is to make the apparent incoming message size different from the apparent outgoing message size to help foil traffic analysis.

In various other embodiments of the invention, a scalable version of the system may be constructed in which a plurality of IP addresses are preassigned to each pair of communicating nodes in the network. Each pair of nodes agrees upon an algorithm for "hopping" between IP addresses (both sending and receiving), such that an eavesdropper sees apparently continuously random IP address pairs (source and destination) for packets transmitted between the pair. Overlapping or "reusable" IP addresses may be allocated to different users on the same subnet, since each node merely verifies that a particular packet includes a valid source/destination pair from the agreed-upon algorithm. Source/destination pairs are preferably not reused between any two nodes during any given end-to-end session, though limited IP block sizes or lengthy sessions might require it.

Further improvements described in this continuation-in-part application include: (1) a load balancer that distributes packets across different transmission paths according to transmission path quality; (2) a DNS proxy server that transparently creates a virtual private network in response to a domain name inquiry; (3) a large-to-small link bandwidth management feature that prevents denial-of-service attacks at system chokepoints; (4) a traffic limiter that regulates incoming packets by limiting the rate at which a transmitter can be synchronized with a receiver; and (5) a signaling synchronizer that allows a large number of nodes to communicate with a central node by partitioning the communication function between two separate entities

The present invention provides key technologies for implementing a secure virtual Internet by using a new agile network protocol that is built on top of the existing Internet protocol (IP). The secure virtual Internet works over the existing Internet infrastructure, and interfaces with client applications the same way as the existing Internet. The key technologies provided by the present invention that support the secure virtual Internet include a "one-click" and "no-click" technique to become part of the secure virtual Internet, a secure domain name service (SDNS) for the secure virtual Internet, and a new approach for interfacing specific client applications onto the secure virtual Internet. According to the invention, the secure domain name service interfaces with existing applications, in addition to providing a way to register and serve domain names and addresses.

According to one aspect of the present invention, a user can conveniently establish a VPN using a "one-click" or a "no-click" technique without being required to enter user identification information, a password and/or an encryption key for establishing a VPN. The advantages of the present invention are provided by a method for establishing a secure communication link between a first computer and a second computer over a computer network, such as the Internet. In one embodiment, a secure communication mode is enabled at a first computer without a user entering any cryptographic information for establishing the secure communication mode of communication, preferably by merely selecting an icon displayed on the first computer. Alternatively, the secure communication mode of communication can be enabled by entering a command into the first computer. Then, a secure communication link is established between the first computer and a second computer over a computer network based on the enabled secure communication mode of communication. According to the invention, it is determined whether a secure communication software module is stored on the first computer in response to the step of enabling the secure communication mode of communication. A predetermined computer network address is then accessed for loading the secure communication software module when the software module is not stored on the first computer. Subsequently, the proxy software module is stored in the first computer. The secure communication link is a virtual private network communication link over the computer network. Preferably, the virtual private network can be based on inserting into each data packet one or more data values that vary according to a pseudo-random

sequence. Alternatively, the virtual private network can be based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses or other data values in packets transmitted between the first computer and the second computer, such that the second computer compares the data values in each data packet transmitted between the first computer and the second computer to a moving window of valid values. Yet another alternative provides that the virtual private network can be based on a comparison between a discriminator field in each data packet to a table of valid discriminator fields maintained for the first computer.

According to another aspect of the invention, a command is entered to define a setup parameter associated with the secure communication link mode of communication. Consequently, the secure communication mode is automatically established when a communication link is established over the computer network.

The present invention also provides a computer system having a communication link to a computer network, and a display showing a hyperlink for establishing a virtual private network through the computer network. When the hyperlink for establishing the virtual private network is selected, a virtual private network is established over the computer network. A non-standard top-level domain name is then sent over the virtual private network communication to a predetermined computer network address, such as a computer network address for a secure domain name service (SDNS).

The present invention provides a domain name service that provides secure computer network addresses for secure, non-standard top-level domain names. The advantages of the present invention are provided by a secure domain name service for a computer network that includes a portal connected to a computer network, such as the Internet, and a domain name database connected to the computer network through the portal. According to the invention, the portal authenticates a query for a secure computer network address, and the domain name database stores secure computer network addresses for the computer network. Each secure computer network address is based on a non-standard top-level domain name, such as .scom, .sorg, .snet, .snet, .sedu, .smil and .sint.

The present invention provides a way to encapsulate existing application network traffic at the application layer of a client computer so that the client application can securely communicate with a server protected by an agile network protocol. The advantages of the present invention are provided by a method for communicating using a private communication link between a client computer and a server computer over a computer network, such as the Internet. According to the invention, an information packet is sent from the client computer to the server computer over the computer network. The information packet contains data that is inserted into the payload portion of the packet at the application layer of the client computer and is used for forming a virtual private connection between the client computer and the server computer. The modified information packet can be sent through a firewall before being sent over the computer network to the server computer and by working on top of existing protocols (i.e., UDP, ICMP and TCP), the present invention more easily penetrates the firewall. The information packet is received at a kernel layer of an operating system on the server side. It is then determined at the kernel layer of the operating system on the host computer whether the information packet contains the data that is used for forming the virtual private connection. The server side replies by sending an information packet to the client computer that has been modified at the kernel layer to containing virtual private connection information in the payload portion of the reply information packet. Preferably, the information packet from the client computer and the reply information packet from the server side are each a UDP protocol information packet. Alternative, both information packets could be a TCP/IP protocol information packet, or an ICMP protocol information packet.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is an illustration of secure communications over the Internet according to a prior art embodiment.

FIG. **2** is an illustration of secure communications over the Internet according to a an embodiment of the invention.

FIG. **3***a* is an illustration of a process of forming a tunneled IP packet according to an embodiment of the invention.

FIG. **3***b* is an illustration of a process of forming a tunneled IP packet according to another embodiment of the invention.

FIG. **4** is an illustration of an OSI layer location of processes that may be used to implement the invention.

FIG. **5** is a flow chart illustrating a process for routing a tunneled packet according to an embodiment of the invention.

FIG. **6** is a flow chart illustrating a process for forming a tunneled packet according to an embodiment of the invention.

FIG. **7** is a flow chart illustrating a process for receiving a tunneled packet according to an embodiment of the invention.

FIG. **8** shows how a secure session is established and synchronized between a client and a TARP router.

FIG. **9** shows an IP address hopping scheme between a client computer and TARP router using transmit and receive tables in each computer.

FIG. **10** shows physical link redundancy among three Internet Service Providers (ISPs) and a client computer.

FIG. **11** shows how multiple IP packets can be embedded into a single "frame" such as an Ethernet frame, and further shows the use of a discriminator field to camouflage true packet recipients.

FIG. **12**A shows a system that employs hopped hardware addresses, hopped IP addresses, and hopped discriminator fields.

FIG. **12**B shows several different approaches for hopping hardware addresses, IP addresses, and discriminator fields in combination.

FIG. **13** shows a technique for automatically re-establishing synchronization between sender and receiver through the use of a partially public sync value.

FIG. **14** shows a "checkpoint" scheme for regaining synchronization between a sender and recipient.

FIG. **15** shows further details of the checkpoint scheme of FIG. **14**.

FIG. **16** shows how two addresses can be decomposed into a plurality of segments for comparison with presence vectors.

FIG. **17** shows a storage array for a receiver's active addresses.

FIG. **18** shows the receiver's storage array after receiving a sync request.

FIG. **19** shows the receiver's storage array after new addresses have been generated.

FIG. **20** shows a system employing distributed transmission paths.

Petitioner Apple Inc. - Exhibit 1002, p. 546

FIG. **21** shows a plurality of link transmission tables that can be used to route packets in the system of FIG. **20**.

FIG. **22**A shows a flowchart for adjusting weight value distributions associated with a plurality of transmission links.

FIG. **22**B shows a flowchart for setting a weight value to zero if a transmitter turns off.

FIG. **23** shows a system employing distributed transmission paths with adjusted weight value distributions for each path.

FIG. **24** shows an example using the system of FIG. **23**.

FIG. **25** shows a conventional domain-name look-up service.

FIG. **26** shows a system employing a DNS proxy server with transparent VPN creation.

FIG. **27** shows steps that can be carried out to implement transparent VPN creation based on a DNS look-up function.

FIG. **28** shows a system including a link guard function that prevents packet overloading on a low-bandwidth link LOW BW.

FIG. **29** shows one embodiment of a system employing the principles of FIG. **28**.

FIG. **30** shows a system that regulates packet transmission rates by throttling the rate at which synchronizations are performed.

FIG. **31** shows a signaling server **3101** and a transport server **3102** used to establish a VPN with a client computer.

FIG. **32** shows message flows relating to synchronization protocols of FIG. **31**.

FIG. **33** shows a system block diagram of a computer network in which the "one-click" secure communication link of the present invention is suitable for use.

FIG. **34** shows a flow diagram for installing and establishing a "one-click" secure communication link over a computer network according to the present invention.

FIG. **35** shows a flow diagram for registering a secure domain name according to the present invention.

FIG. **36** shows a system block diagram of a computer network in which a private connection according to the present invention can be configured to more easily traverse a firewall between two computer networks.

FIG. **37** shows a flow diagram for establishing a virtual private connection that is encapsulated using an existing network protocol.

DETAILED DESCRIPTION OF THE INVENTION

Referring to FIG. **2**, a secure mechanism for communicating over the internet employs a number of special routers or servers, called TARP routers **122–127** that are similar to regular IP routers **128–132** in that each has one or more IP addresses and uses normal IP protocol to send normal-looking IP packet messages, called TARP packets **140**. TARP packets **140** are identical to normal IP packet messages that are routed by regular IP routers **128–132** because each TARP packet **140** contains a destination address as in a normal IP packet. However, instead of indicating a final destination in the destination field of the IP header, the TARP packet's **140** IP header always points to a next-hop in a series of TARP router hops, or the final destination, TARP terminal **110**. Because the header of the TARP packet contains only the next-hop destination, there is no overt indication from an intercepted TARP packet of the true destination of the TARP packet **140** since the destination could always be the next-hop TARP router as well as the final destination, TARP terminal **110**.

Each TARP packet's true destination is concealed behind an outer layer of encryption generated using a link key **146**. The link key **146** is the encryption key used for encrypted communication between the end points (TARP terminals or TARP routers) of a single link in the chain of hops connecting the originating TARP terminal **100** and the destination TARP terminal **110**. Each TARP router **122–127**, using the link key **146** it uses to communicate with the previous hop in a chain, can use the link key to reveal the true destination of a TARP packet. To identify the link key needed to decrypt the outer layer of encryption of a TARP packet, a receiving TARP or routing terminal may identify the transmitting terminal (which may indicate the link key used) by the sender field of the clear IP header. Alternatively, this identity may be hidden behind another layer of encryption in available bits in the clear IP header. Each TARP router, upon receiving a TARP message, determines if the message is a TARP message by using authentication data in the TARP packet. This could be recorded in available bytes in the TARP packet's IP header. Alternatively, TARP packets could be authenticated by attempting to decrypt using the link key **146** and determining if the results are as expected. The former may have computational advantages because it does not involve a decryption process.

Once the outer layer of decryption is completed by a TARP router **122–127**, the TARP router determines the final destination. The system is preferably designed to cause each TARP packet **140** to undergo a minimum number of hops to help foil traffic analysis. The time to live counter in the IP header of the TARP message may be used to indicate a number of TARP router hops yet to be completed. Each TARP router then would decrement the counter and determine from that whether it should forward the TARP packet **140** to another TARP router **122–127** or to the destination TARP terminal **110**. If the time to live counter is zero or below zero after decrementing, for an example of usage, the TARP router receiving the TARP packet **140** may forward the TARP packet **140** to the destination TARP terminal **110**. If the time to live counter is above zero after decrementing, for an example of usage, the TARP router receiving the TARP packet **140** may forward the TARP packet **140** to a TARP router **122 127** that the current TARP terminal chooses at random. As a result, each TARP packet **140** is routed through some minimum number of hops of TARP routers **122–127** which are chosen at random.

Thus, each TARP packet, irrespective of the traditional factors determining traffic in the Internet, makes random trips among a number of geographically disparate routers before reaching its destination and each trip is highly likely to be different for each packet composing a given message because each trip is independently randomly determined as described above. This feature is called agile routing. For reasons that will become clear shortly, the fact that different packets take different routes provides distinct advantages by making it difficult for an interloper to obtain all the packets forming an entire multi-packet message. Agile routing is combined with another feature that furthers this purpose, a feature that ensures that any message is broken into multiple packets.

A TARP router receives a TARP packet when an IP address used by the TARP router coincides with the IP address in the TARP packet's IP header IP_C. The IP address of a TARP router, however, may not remain constant. To avoid and manage attacks, each TARP router, independently or under direction from another TARP terminal or router, may change its IP address. A separate, unchangeable identifier or address is also defined. This address, called the

TARP address, is known only to TARP routers and terminals and may be correlated at any time by a TARP router or a TARP terminal using a Lookup Table (LUT). When a TARP router or terminal changes its IP address, it updates the other TARP routers and terminals which in turn update their respective LUTs. In reality, whenever a TARP router looks up the address of a destination in the encrypted header, it must convert a TARP address to a real IP address using its LUT.

While every TARP router receiving a TARP packet has the ability to determine the packet's final destination, the message payload is embedded behind an inner layer of encryption in the TARP packet that can only be unlocked using a session key. The session key is not available to any of the TARP routers **122–127** intervening between the originating **100** and destination **110** TARP terminals. The session key is used to decrypt the payloads of the TARP packets **140** permitting an entire message to be reconstructed.

In one embodiment, communication may be made private using link and session keys, which in turn may be shared and used according any desired method. For example, a public key or symmetric keys may be communicated between link or session endpoints using a public key method. Any of a variety of other mechanisms for securing data to ensure that only authorized computers can have access to the private information in the TARP packets **140** may be used as desired.

Referring to FIG. **3***a*, to construct a series of TARP packets, a data stream **300** of IP packets **207***a*, **207***b*, **207***c*, etc., such series of packets being formed by a network (IP) layer process, is broken into a series of small sized segments. In the present example, equal-sized segments **1–9** are defined and used to construct a set of interleaved data packets A, B, and C. Here it is assumed that the number of interleaved packets A, B, and C formed is three and that the number of IP packets **207***a*–**207***c* used to form the three interleaved packets A, B, and C is exactly three. Of course, the number of IP packets spread over a group of interleaved packets may be any convenient number as may be the number of interleaved packets over which the incoming data stream is spread. The latter, the number of interleaved packets over which the data stream is spread, is called the interleave window.

To create a packet, the transmitting software interleaves the normal IP packets **207***a* et. seq. to form a new set of interleaved payload data **320**. This payload data **320** is then encrypted using a session key to form a set of session-key-encrypted payload data **330**, each of which, A, B, and C, will form the payload of a TARP packet. Using the IP header data, from the original packets **207***a*–**207***c*, new TARP headers IP_T are formed. The TARP headers IP_T can be identical to normal IP headers or customized in some way. In a preferred embodiment, the TARP headers IP_T are IP headers with added data providing the following information required for routing and reconstruction of messages, some of which data is ordinarily, or capable of being, contained in normal IP headers:

1. A window sequence number—an identifier that indicates where the packet belongs in the original message sequence.
2. An interleave sequence number—an identifier that indicates the interleaving sequence used to form the packet so that the packet can be deinterleaved along with other packets in the interleave window.
3. A time-to-live (TTL) datum—indicates the number of TARP-router-hops to be executed before the packet reaches its destination. Note that the TTL parameter may provide a datum to be used in a probabilistic formula for determining whether to route the packet to the destination or to another hop.
4. Data type identifier—indicates whether the payload contains, for example, TCP or UDP data.
5. Sender's address—indicates the sender's address in the TARP network.
6. Destination address—indicates the destination terminal's address in the TARP network.
7. Decoy/Real—an indicator of whether the packet contains real message data or dummy decoy data or a combination.

Obviously, the packets going into a single interleave window must include only packets with a common destination. Thus, it is assumed in the depicted example that the IP headers of IP packets **207***a*–**207***c* all contain the same destination address or at least will be received by the same terminal so that they can be deinterleaved. Note that dummy or decoy data or packets can be added to form a larger interleave window than would otherwise be required by the size of a given message. Decoy or dummy data can be added to a stream to help foil traffic analysis by leveling the load on the network. Thus, it may be desirable to provide the TARP process with an ability to respond to the time of day or other criteria to generate more decoy data during low traffic periods so that communication bursts at one point in the Internet cannot be tied to communication bursts at another point to reveal the communicating endpoints.

Dummy data also helps to break the data into a larger number of inconspicuously-sized packets permitting the interleave window size to be increased while maintaining a reasonable size for each packet. (The packet size can be a single standard size or selected from a fixed range of sizes.) One primary reason for desiring for each message to be broken into multiple packets is apparent if a chain block encryption scheme is used to form the first encryption layer prior to interleaving. A single block encryption may be applied to a portion, or the entirety, of a message, and that portion or entirety then interleaved into a number of separate packets.

Referring to FIG. **3***b*, in an alternative mode of TARP packet construction, a series of IP packets are accumulated to make up a predefined interleave window. The payloads of the packets are used to construct a single block **520** for chain block encryption using the session key. The payloads used to form the block are presumed to be destined for the same terminal. The block size may coincide with the interleave window as depicted in the example embodiment of FIG. **3***b*. After encryption, the encrypted block is broken into separate payloads and segments which are interleaved as in the embodiment of FIG. **3***a*. The resulting interleaved packets A, B, and C, are then packaged as TARP packets with TARP headers as in the Example of FIG. **3***a*. The remaining process is as shown in, and discussed with reference to, FIG. **3***a*.

Once the TARP packets **340** are formed, each entire TARP packet **340**, including the TARP header IP_T, is encrypted using the link key for communication with the first-hop-TARP router. The first hop TARP router is randomly chosen. A final unencrypted IP header IPC is added to each encrypted TARP packet **340** to form a normal IP packet **360** that can be transmitted to a TARP router. Note that the process of constructing the TARP packet **360** does not have to be done in stages as described. The above description is just a useful heuristic for describing the final product, namely, the TARP packet.

Note that, TARP header IP_T could be a completely custom header configuration with no similarity to a normal IP header except that it contain the information identified above. This is so since this header is interpreted by only TARP routers.

The above scheme may be implemented entirely by processes operating between the data link layer and the network layer of each server or terminal participating in the TARP system. Referring to FIG. **4**, a TARP transceiver **405** can be an originating terminal **100**, a destination terminal **110**, or a TARP router **122** . . . **127**. In each TARP Transceiver **405**, a transmitting process is generated to receive normal packets from the Network (IP) layer and generate TARP packets for communication over the network. A receiving process is generated to receive normal IP packets containing TARP packets and generate from these normal IP packets which are "passed up" to the Network (IP) layer. Note that where the TARP Transceiver **405** is a router, the received TARP packets **140** are not processed into a stream of IP packets **415** because they need only be authenticated as proper TARP packets and then passed to another TARP router or a TARP destination terminal **110**. The intervening process, a "TARP Layer" **420**, could be combined with either the data link layer **430** or the Network layer **410**. In either case, it would intervene between the data link layer **430** so that the process would receive regular IP packets containing embedded TARP packets and "hand up" a series of reassembled IP packets to the Network layer **410**. As an example of combining the TARP layer **420** with the data link layer **430**, a program may augment the normal processes running a communications card, for example, an Ethernet card. Alternatively, the TARP layer processes may form part of a dynamically loadable module that is loaded and executed to support communications between the network and data link layers.

Because the encryption system described above can be inserted between the data link and network layers, the processes involved in supporting the encrypted communication may be completely transparent to processes at the IP (network) layer and above. The TARP processes may also be completely transparent to the data link layer processes as well. Thus, no operations at or above the network layer, or at or below the data link layer, are affected by the insertion of the TARP stack. This provides additional security to all processes at or above the network layer, since the difficulty of unauthorized penetration of the network layer (by, for example, a hacker) is increased substantially. Even newly developed servers running at the session layer leave all processes below the session layer vulnerable to attack. Note that in this architecture, security is distributed. That is, notebook computers used by executives on the road, for example, can communicate over the Internet without any compromise in security.

Note that IP address changes made by TARP terminals and routers can be done at regular intervals, at random intervals, or upon detection of "attacks." The variation of IP addresses hinders traffic analysis that might reveal which computers are communicating, and also provides a degree of immunity from attack. The level of immunity from attack is roughly proportional to the rate at which the IP address of the host is changing. As mentioned, IP addresses may be changed in response to attacks. An attack may be revealed, for example, by a regular series of messages indicates that a router is being probed in some way. Upon detection of an attack, the TARP layer process may respond to this event by changing its IP address. To accomplish this, the TARP process will construct a TARP-formatted message, in the style of Internet Control Message Protocol (ICMP) datagrams as an example; this message will contain the machine's TARP address, its previous IP address, and its new IP address. The TARP layer will transmit this packet to at least one known TARP router; then upon receipt and validation of the message, the TARP router will update its LUT with the new IP address for the stated TARP address. The TARP router will then format a similar message, and broadcast it to the other TARP routers so that they may update their LUTs. Since the total number of TARP routers on any given subnet is expected to be relatively small, this process of updating the LUTs should be relatively fast. It may not, however, work as well when there is a relatively large number of TARP routers and/or a relatively large number of clients; this has motivated a refinement of this architecture to provide scalability; this refinement has led to a second embodiment, which is discussed below.

Upon detection of an attack, the TARP process may also create a subprocess that maintains the original IP address and continues interacting with the attacker. The latter may provide an opportunity to trace the attacker or study the attacker's methods (called "fishbowling" drawing upon the analogy of a small fish in a fish bowl that "thinks" it is in the ocean but is actually under captive observation). A history of the communication between the attacker and the abandoned (fishbowled) IP address can be recorded or transmitted for human analysis or further synthesized for purposes of responding in some way.

As mentioned above, decoy or dummy data or packets can be added to outgoing data streams by TARP terminals or routers. In addition to making it convenient to spread data over a larger number of separate packets, such decoy packets can also help to level the load on inactive portions of the Internet to help foil traffic analysis efforts.

Decoy packets may be generated by each TARP terminal **100, 110** or each router **122–127** on some basis determined by an algorithm. For example, the algorithm may be a random one which calls for the generation of a packet on a random basis when the terminal is idle. Alternatively, the algorithm may be responsive to time of day or detection of low traffic to generate more decoy packets during low traffic times. Note that packets are preferably generated in groups, rather than one by one, the groups being sized to simulate real messages. In addition, so that decoy packets may be inserted in normal TARP message streams, the background loop may have a latch that makes it more likely to insert decoy packets when a message stream is being received. That is, when a series of messages are received, the decoy packet generation rate may be increased. Alternatively, if a large number of decoy packets is received along with regular TARP packets, the algorithm may increase the rate of dropping of decoy packets rather than forwarding them. The result of dropping and generating decoy packets in this way is to make the apparent incoming message size different from the apparent outgoing message size to help foil traffic analysis. The rate of reception of packets, decoy or otherwise, may be indicated to the decoy packet dropping and generating processes through perishable decoy and regular packet counters. (A perishable counter is one that resets or decrements its value in response to time so that it contains a high value when it is incremented in rapid succession and a small value when incremented either slowly or a small number of times in rapid succession.) Note that destination TARP terminal **110** may generate decoy packets equal in number and size to those TARP packets received to make it appear it is merely routing packets and is therefore not the destination terminal.

Referring to FIG. 5, the following particular steps may be employed in the above-described method for routing TARP packets.

S0. A background loop operation is performed which applies an algorithm which determines the generation of decoy IP packets. The loop is interrupted when an encrypted TARP packet is received.

S2. The TARP packet may be probed in some way to authenticate the packet before attempting to decrypt it using the link key. That is, the router may determine that the packet is an authentic TARP packet by performing a selected operation on some data included with the clear IP header attached to the encrypted TARP packet contained in the payload. This makes it possible to avoid performing decryption on packets that are not authentic TARP packets.

S3. The TARP packet is decrypted to expose the destination TARP address and an indication of whether the packet is a decoy packet or part of a real message.

S4. If the packet is a decoy packet, the perishable decoy counter is incremented.

S5. Based on the decoy generation/dropping algorithm and the perishable decoy counter value, if the packet is a decoy packet, the router may choose to throw it away. If the received packet is a decoy packet and it is determined that it should be thrown away (S6), control returns to step S0.

S7. The TTL parameter of the TARP header is decremented and it is determined if the TTL parameter is greater than zero.

S8. If the TTL parameter is greater than zero, a TARP address is randomly chosen from a list of TARP addresses maintained by the router and the link key and IP address corresponding to that TARP address memorized for use in creating a new IP packet containing the TARP packet.

S9. If the TTL parameter is zero or less, the link key and IP address corresponding to the TARP address of the destination are memorized for use in creating the new IP packet containing the TARP packet.

S10. The TARP packet is encrypted using the memorized link key.

S11. An IP header is added to the packet that contains the stored IP address, the encrypted TARP packet wrapped with an IP header, and the completed packet transmitted to the next hop or destination.

Referring to FIG. 6, the following particular steps may be employed in the above-described method for generating TARP packets.

S20. A background loop operation applies an algorithm that determines the generation of decoy IP packets. The loop is interrupted when a data stream containing IP packets is received for transmission.

S21. The received IP packets are grouped into a set consisting of messages with a constant IP destination address. The set is further broken down to coincide with a maximum size of an interleave window The set is encrypted, and interleaved into a set of payloads destined to become TARP packets.

S22. The TARP address corresponding to the IP address is determined from a lookup table and stored to generate the TARP header. An initial TTL count is generated and stored in the header. The TTL count may be random with minimum and maximum values or it may be fixed or determined by some other parameter.

S23. The window sequence numbers and interleave sequence numbers are recorded in the TARP headers of each packet.

S24. One TARP router address is randomly chosen for each TARP packet and the IP address corresponding to it stored for use in the clear IP header. The link key corresponding to this router is identified and used to encrypt TARP packets containing interleaved and encrypted data and TARP headers.

S25. A clear IP header with the first hop router's real IP address is generated and added to each of the encrypted TARP packets and the resulting packets.

Referring to FIG. 7, the following particular steps may be employed in the above-described method for receiving TARP packets.

S40. A background loop operation is performed which applies an algorithm which determines the generation of decoy IP packets. The loop is interrupted when an encrypted TARP packet is received.

S42. The TARP packet may be probed to authenticate the packet before attempting to decrypt it using the link key.

S43. The TARP packet is decrypted with the appropriate link key to expose the destination TARP address and an indication of whether the packet is a decoy packet or part of a real message.

S44. If the packet is a decoy packet, the perishable decoy counter is incremented.

S45. Based on the decoy generation/dropping algorithm and the perishable decoy counter value, if the packet is a decoy packet, the receiver may choose to throw it away.

S46. The TARP packets are cached until all packets forming an interleave window are received.

S47. Once all packets of an interleave window are received, the packets are deinterleaved.

S48. The packets block of combined packets defining the interleave window is then decrypted using the session key.

S49. The decrypted block is then divided using the window sequence data and the IP_I headers are converted into normal IP_C headers. The window sequence numbers are integrated in the IP_C headers.

S50. The packets are then handed up to the IP layer processes.

1. Scalability Enhancements

The IP agility feature described above relies on the ability to transmit IP address changes to all TARP routers. The embodiments including this feature will be referred to as "boutique" embodiments due to potential limitations in scaling these features up for a large network, such as the Internet. (The "boutique" embodiments would, however, be robust for use in smaller networks, such as small virtual private networks, for example). One problem with the boutique embodiments is that if IP address changes are to occur frequently, the message traffic required to update all routers sufficiently quickly creates a serious burden on the Internet when the TARP router and/or client population gets large. The bandwidth burden added to the networks, for example in ICMP packets, that would be used to update all the TARP routers could overwhelm the Internet for a large scale implementation that approached the scale of the Internet. In other words, the boutique system's scalability is limited.

A system can be constructed which trades some of the features of the above embodiments to provide the benefits of IP agility without the additional messaging burden. This is accomplished by IP address-hopping according to shared algorithms that govern IP addresses used between links participating in communications sessions between nodes such as TARP nodes. (Note that the IP hopping technique is

also applicable to the boutique embodiment.) The IP agility feature discussed with respect to the boutique system can be modified so that it becomes decentralized under this scalable regime and governed by the above-described shared algorithm. Other features of the boutique system may be combined with this new type of IP-agility.

The new embodiment has the advantage of providing IP agility governed by a local algorithm and set of IP addresses exchanged by each communicating pair of nodes. This local governance is session-independent in that it may govern communications between a pair of nodes, irrespective of the session or end points being transferred between the directly communicating pair of nodes.

In the scalable embodiments, blocks of IP addresses are allocated to each node in the network. (This scalability will increase in the future, when Internet Protocol addresses are increased to 128-bit fields, vastly increasing the number of distinctly addressable nodes). Each node can thus use any of the IP addresses assigned to that node to communicate with other nodes in the network. Indeed, each pair of communicating nodes can use a plurality of source IP addresses and destination IP addresses for communicating with each other.

Each communicating pair of nodes in a chain participating in any session stores two blocks of IP addresses, called netblocks, and an algorithm and randomization seed for selecting, from each netblock, the next pair of source/destination IP addresses that will be used to transmit the next message. In other words, the algorithm governs the sequential selection of IP-address pairs, one sender and one receiver IP address, from each netblock. The combination of algorithm, seed, and netblock (IP address block) will be called a "hopblock." A router issues separate transmit and receive hopblocks to its clients. The send address and the receive address of the IP header of each outgoing packet sent by the client are filled with the send and receive IP addresses generated by the algorithm. The algorithm is "clocked" (indexed) by a counter so that each time a pair is used, the algorithm turns out a new transmit pair for the next packet to be sent.

The router's receive hopblock is identical to the client's transmit hopblock. The router uses the receive hopblock to predict what the send and receive IP address pair for the next expected packet from that client will be. Since packets can be received out of order, it is not possible for the router to predict with certainty what IP address pair will be on the next sequential packet. To account for this problem, the router generates a range of predictions encompassing the number of possible transmitted packet send/receive addresses, of which the next packet received could leap ahead. Thus, if there is a vanishingly small probability that a given packet will arrive at the router ahead of 5 packets transmitted by the client before the given packet, then the router can generate a series of 6 send/receive IP address pairs (or "hop window") to compare with the next received packet. When a packet is received, it is marked in the hop window as such, so that a second packet with the same IP address pair will be discarded. If an out-of-sequence packet does not arrive within a predetermined timeout period, it can be requested for retransmission or simply discarded from the receive table, depending upon the protocol in use for that communications session, or possibly by convention.

When the router receives the client's packet, it compares the send and receive IP addresses of the packet with the next N predicted send and receive IP address pairs and rejects the packet if it is not a member of this set. Received packets that do not have the predicted source/destination IP addresses falling with the window are rejected, thus thwarting possible hackers. (With the number of possible combinations, even a fairly large window would be hard to fall into at random.) If it is a member of this set, the router accepts the packet and processes it further. This link-based IP-hopping strategy, referred to as "IHOP," is a network element that stands on its own and is not necessarily accompanied by elements of the boutique system described above. If the routing agility feature described in connection with the boutique embodiment is combined with this link-based IP-hopping strategy, the router's next step would be to decrypt the TARP header to determine the destination TARP router for the packet and determine what should be the next hop for the packet. The TARP router would then forward the packet to a random TARP router or the destination TARP router with which the source TARP router has a link-based IP hopping communication established.

FIG. **8** shows how a client computer **801** and a TARP router **811** can establish a secure session. When client **801** seeks to establish an IHOP session with TARP router **811**, the client **801** sends "secure synchronization" request ("SSYN") packet **821** to the TARP router **811**. This SYN packet **821** contains the client's **801** authentication token, and may be sent to the router **811** in an encrypted format. The source and destination IP numbers on the packet **821** are the client's **801** current fixed IP address, and a "known" fixed IP address for the router **811**. (For security purposes, it may be desirable to reject any packets from outside of the local network that are destined for the router's known fixed IP address.) Upon receipt and validation of the client's **801** SSYN packet **821**, the router **811** responds by sending an encrypted "secure synchronization acknowledgment" ("SSYN ACK") **822** to the client **801**. This SSYN ACK **822** will contain the transmit and receive hopblocks that the client **801** will use when communicating with the TARP router **811**. The client **801** will acknowledge the TARP router's **811** response packet **822** by generating an encrypted SSYN ACK ACK packet **823** which will be sent from the client's **801** fixed IP address and to the TARP router's **811** known fixed IP address. The client **801** will simultaneously generate a SSYN ACK ACK packet; this SSYN ACK packet, referred to as the Secure Session Initiation (SSI) packet **824**, will be sent with the first {sender, receiver} IP pair in the client's transmit table **921** (FIG. **9**), as specified in the transmit hopblock provided by the TARP router **811** in the SSYN ACK packet **822**. The TARP router **811** will respond to the SSI packet **824** with an SSI ACK packet **825**, which will be sent with the first {sender, receiver} IP pair in the TARP router's transmit table **923**. Once these packets have been successfully exchanged, the secure communications session is established, and all further secure communications between the client **801** and the TARP router **811** will be conducted via this secure session, as long as synchronization is maintained. If synchronization is lost, then the client **801** and TARP router **802** may re-establish the secure session by the procedure outlined in FIG. **8** and described above.

While the secure session is active, both the client **901** and TARP router **911** (FIG. **9**) will maintain their respective transmit tables **921**, **923** and receive tables **922**, **924**, as provided by the TARP router during session synchronization **822**. It is important that the sequence of IP pairs in the client's transmit table **921** be identical to those in the TARP router's receive table **924**; similarly, the sequence of IP pairs in the client's receive table **922** must be identical to those in the router's transmit table **923**. This is required for the session synchronization to be maintained. The client **901** need maintain only one transmit table **921** and one receive

Petitioner Apple Inc. - Exhibit 1002, p. 551

table **922** during the course of the secure session. Each sequential packet sent by the client **901** will employ the next {send, receive} IP address pair in the transmit table, regardless of TCP or UDP session. The TARP router **911** will expect each packet arriving from the client **901** to bear the next IP address pair shown in its receive table.

Since packets can arrive out of order, however, the router **911** can maintain a "look ahead" buffer in its receive table, and will mark previously-received IP pairs as invalid for future packets; any future packet containing an IP pair that is in the look-ahead buffer but is marked as previously received will be discarded. Communications from the TARP router **911** to the client **901** are maintained in an identical manner; in particular, the router **911** will select the next IP address pair from its transmit table **923** when constructing a packet to send to the client **901**, and the client **901** will maintain a look-ahead buffer of expected IP pairs on packets that it is receiving. Each TARP router will maintain separate pairs of transmit and receive tables for each client that is currently engaged in a secure session with or through that TARP router.

While clients receive their hopblocks from the first server linking them to the Internet, routers exchange hopblocks. When a router establishes a link-based IP-hopping communication regime with another router, each router of the pair exchanges its transmit hopblock. The transmit hopblock of each router becomes the receive hopblock of the other router. The communication between routers is governed as described by the example of a client sending a packet to the first router.

While the above strategy works fine in the IP milieu, many local networks that are connected to the Internet are Ethernet systems. In Ethernet, the IP addresses of the destination devices must be translated into hardware addresses, and vice versa, using known processes ("address resolution protocol," and "reverse address resolution protocol"). However, if the link-based IP-hopping strategy is employed, the correlation process would become explosive and burdensome. An alternative to the link-based IP hopping strategy may be employed within an Ethernet network. The solution is to provide that the node linking the Internet to the Ethernet (call it the border node) use the link-based IP-hopping communication regime to communicate with nodes outside the Ethernet LAN. Within the Ethernet LAN, each TARP node would have a single IP address which would be addressed in the conventional way. Instead of comparing the {sender, receiver} IP address pairs to authenticate a packet, the intra-LAN TARP node would use one of the IP header extension fields to do so. Thus, the border node uses an algorithm shared by the intra-LAN TARP node to generate a symbol that is stored in the free field in the IP header, and the intra-LAN TARP node generates a range of symbols based on its prediction of the next expected packet to be received from that particular source IP address. The packet is rejected if it does not fall into the set of predicted symbols (for example, numerical values) or is accepted if it does. Communications from the intra-LAN TARP node to the border node are accomplished in the same manner, though the algorithm will necessarily be different for security reasons. Thus, each of the communicating nodes will generate transmit and receive tables in a similar manner to that of FIG. **9**; the intra-LAN TARP nodes transmit table will be identical to the border node's receive table, and the intra-LAN TARP node's receive table will be identical to the border node's transmit table.

The algorithm used for IP address-hopping can be any desired algorithm. For example, the algorithm can be a given pseudo-random number generator that generates numbers of the range covering the allowed IP addresses with a given seed. Alternatively, the session participants can assume a certain type of algorithm and specify simply a parameter for applying the algorithm. For example the assumed algorithm could be a particular pseudo-random number generator and the session participants could simply exchange seed values.

Note that there is no permanent physical distinction between the originating and destination terminal nodes. Either device at either end point can initiate a synchronization of the pair. Note also that the authentication/synchronization-request (and acknowledgment) and hopblock-exchange may all be served by a single message so that separate message exchanges may not be required.

As another extension to the stated architecture, multiple physical paths can be used by a client, in order to provide link redundancy and further thwart attempts at denial of service and traffic monitoring. As shown in FIG. **10**, for example, client **1001** can establish three simultaneous sessions with each of three TARP routers provided by different ISPs **1011**, **1012**, **1013**. As an example, the client **1001** can use three different telephone lines **1021**, **1022**, **1023** to connect to the ISPs, or two telephone lines and a cable modem, etc. In this scheme, transmitted packets will be sent in a random fashion among the different physical paths. This architecture provides a high degree of communications redundancy, with improved immunity from denial-of-service attacks and traffic monitoring.

2. Further Extensions

The following describes various extensions to the techniques, systems, and methods described above. As described above, the security of communications occurring between computers in a computer network (such as the Internet, an Ethernet, or others) can be enhanced by using seemingly random source and destination Internet Protocol (IP) addresses for data packets transmitted over the network. This feature prevents eavesdroppers from determining which computers in the network are communicating with each other while permitting the two communicating computers to easily recognize whether a given received data packet is legitimate or not. In one embodiment of the above-described systems, an IP header extension field is used to authenticate incoming packets on an Ethernet.

Various extensions to the previously described techniques described herein include: (1) use of hopped hardware or "MAC" addresses in broadcast type network; (2) a self-synchronization technique that permits a computer to automatically regain synchronization with a sender; (3) synchronization algorithms that allow transmitting and receiving computers to quickly re-establish synchronization in the event of lost packets or other events; and (4) a fast-packet rejection mechanism for rejecting invalid packets. Any or all of these extensions can be combined with the features described above in any of various ways.

A. Hardware Address Hopping

Internet protocol-based communications techniques on a LAN or across any dedicated physical medium-typically embed the IP packets within lower-level packets, often referred to as "frames." As shown in FIG. **11**, for example, a first Ethernet frame **1150** comprises a frame header **1101** and two embedded IP packets IP1 and IP2, while a second Ethernet frame **1160** comprises a different frame header **1104** and a single IP packet IP3. Each frame header gener-

ally includes a source hardware address **1101A** and a destination hardware address **1101B**; other well-known fields in frame headers are omitted from FIG. **11** for clarity. Two hardware nodes communicating over a physical communication channel insert appropriate source and destination hardware addresses to indicate which nodes on the channel or network should receive the frame.

It may be possible for a nefarious listener to acquire information about the contents of a frame and/or its communicants by examining frames on a local network rather than (or in addition to) the IP packets themselves. This is especially true in broadcast media, such as Ethernet, where it is necessary to insert into the frame header the hardware address of the machine that generated the frame and the hardware address of the machine to which frame is being sent. All nodes on the network can potentially "see" all packets transmitted across the network. This can be a problem for secure communications, especially in cases where the communicants do not want for any third party to be able to identify who is engaging in the information exchange. One way to address this problem is to push the address-hopping scheme down to the hardware layer. In accordance with various embodiments of the invention, hardware addresses are "hopped" in a manner similar to that used to change IP addresses, such that a listener cannot determine which hardware node generated a particular message nor which node is the intended recipient.

FIG. **12**A shows a system in which Media Access Control ("MAC") hardware addresses are "hopped" in order to increase security over a network such as an Ethernet. While the description refers to the exemplary case of an Ethernet environment, the inventive principles are equally applicable to other types of communications media. In the Ethernet case, the MAC address of the sender and receiver are inserted into the Ethernet frame and can be observed by anyone on the LAN who is within the broadcast range for that frame. For secure communications, it becomes desirable to generate frames with MAC addresses that are not attributable to any specific sender or receiver.

As shown in FIG. 12A, two computer nodes **1201** and **1202** communicate over a communication channel such as an Ethernet. Each node executes one or more application programs **1203** and **1218** that communicate by transmitting packets through communication software **1204** and **1217**, respectively. Examples of application programs include video conferencing, e-mail, word processing programs, telephony, and the like. Communication software **1204** and **1217** can comprise, for example, an OSI layered architecture or "stack" that standardizes various services provided at different levels of functionality.

The lowest levels of communication software **1204** and **1217** communicate with hardware components **1206** and **1214** respectively, each of which can include one or more registers **1207** and **1215** that allow the hardware to be reconfigured or controlled in accordance with various communication protocols. The hardware components (an Ethernet network interface card, for example) communicate with each other over the communication medium. Each hardware component is typically pre-assigned a fixed hardware address or MAC number that identifies the hardware component to other nodes on the network. One or more interface drivers control the operation of each card and can, for example, be configured to accept or reject packets from certain hardware addresses. As will be described in more detail below, various embodiments of the inventive principles provide for "hopping" different addresses using one or more algorithms and one or more moving windows that track a range of valid addresses to validate received packets. Packets transmitted according to one or more of the inventive principles will be generally referred to as "secure" packets or "secure communications" to differentiate them from ordinary data packets that are transmitted in the clear using ordinary, machine-correlated addresses.

One straightforward method of generating non-attributable MAC addresses is an extension of the IP hopping scheme. In this scenario, two machines on the same LAN that desire to communicate in a secure fashion exchange random-number generators and seeds, and create sequences of quasi-random MAC addresses for synchronized hopping. The implementation and synchronization issues are then similar to that of IP hopping.

This approach, however, runs the risk of using MAC addresses that are currently active on the LAN—which, in turn, could interrupt communications for those machines. Since an Ethernet MAC address is at present 48 bits in length, the chance of randomly misusing an active MAC address is actually quite small. However, if that figure is multiplied by a large number of nodes (as would be found on an extensive LAN), by a large number of frames (as might be the case with packet voice or streaming video), and by a large number of concurrent Virtual Private Networks (VPNs), then the chance that a non-secure machine's MAC address could be used in an address-hopped frame can become non-trivial. In short, any scheme that runs even a small risk of interrupting communications for other machines on the LAN is bound to receive resistance from prospective system administrators. Nevertheless, it is technically feasible, and can be implemented without risk on a LAN on which there is a small number of machines, or if all of the machines on the LAN are engaging in MAC-hopped communications.

Synchronized MAC address hopping may incur some overhead in the course of session establishment, especially if there are multiple sessions or multiple nodes involved in the communications. A simpler method of randomizing MAC addresses is to allow each node to receive and process every incident frame on the network. Typically, each network interface driver will check the destination MAC address in the header of every incident frame to see if it matches that machine's MAC address; if there is no match, then the frame is discarded. In one embodiment, however, these checks can be disabled, and every incident packet is passed to the TARP stack for processing. This will be referred to as "promiscuous" mode, since every incident frame is processed. Promiscuous mode allows the sender to use completely random, unsynchronized MAC addresses, since the destination machine is guaranteed to process the frame. The decision as to whether the packet was truly intended for that machine is handled by the TARP stack, which checks the source and destination IP addresses for a match in its IP synchronization tables. If no match is found, the packet is discarded; if there is a match, the packet is unwrapped, the inner header is evaluated, and if the inner header indicates that the packet is destined for that machine then the packet is forwarded to the IP stack otherwise it is discarded.

One disadvantage of purely-random MAC address hopping is its impact on processing overhead; that is, since every incident frame must be processed, the machine's CPU is engaged considerably more often than if the network interface driver is discriminating and rejecting packets unilaterally. A compromise approach is to select either a single fixed MAC address or a small number of MAC addresses (e.g., one for each virtual private network on an Ethernet) to

use for MAC-hopped communications, regardless of the actual recipient for which the message is intended. In this mode, the network interface driver can check each incident frame against one (or a few) pre-established MAC addresses, thereby freeing the CPU from the task of physical-layer packet discrimination. This scheme does not betray any useful information to an interloper on the LAN; in particular, every secure packet can already be identified by a unique packet type in the outer header. However, since all machines engaged in secure communications would either be using the same MAC address, or be selecting from a small pool of predetermined MAC addresses, the association between a specific machine and a specific MAC address is effectively broken.

In this scheme, the CPU will be engaged more often than it would be in non-secure communications (or in synchronized MAC address hopping), since the network interface driver cannot always unilaterally discriminate between secure packets that are destined for that machine, and secure packets from other VPNs. However, the non-secure traffic is easily eliminated at the network interface, thereby reducing the amount of processing required of the CPU. There are boundary conditions where these statements would not hold, of course—e.g., if all of the traffic on the LAN is secure traffic, then the CPU would be engaged to the same degree as it is in the purely-random address hopping case; alternatively, if each VPN on the LAN uses a different MAC address, then the network interface can perfectly discriminate secure frames destined for the local machine from those constituting other VPNs. These are engineering tradeoffs that might be best handled by providing administrative options for the users when installing the software and/or establishing VPNs.

Even in this scenario, however, there still remains a slight risk of selecting MAC addresses that are being used by one or more nodes on the LAN. One solution to this problem is to formally assign one address or a range of addresses for use in MAC-hopped communications. This is typically done via an assigned numbers registration authority; e.g., in the case of Ethernet, MAC address ranges are assigned to vendors by the Institute of Electrical and Electronics Engineers (IEEE). A formally-assigned range of addresses would ensure that secure frames do not conflict with any properly-configured and properly-functioning machines on the LAN.

Reference will now be made to FIGS. **12**A and **12**B in order to describe the many combinations and features that follow the inventive principles. As explained above, two computer nodes **1201** and **1202** are assumed to be communicating over a network or communication medium such as an Ethernet. A communication protocol in each node (**1204** and **1217**, respectively) contains a modified element **1205** and **1216** that performs certain functions that deviate from the standard communication protocols. In particular, computer node **1201** implements a first "hop" algorithm **1208**X that selects seemingly random source and destination IP addresses (and, in one embodiment, seemingly random IP header discriminator fields) in order to transmit each packet to the other computer node. For example, node **1201** maintains a transmit table **1208** containing triplets of source (S), destination (D), and discriminator fields (DS) that are inserted into outgoing IP packet headers. The table is generated through the use of an appropriate algorithm (e.g., a random number generator that is seeded with an appropriate seed) that is known to the recipient node **1202**. As each new IP packet is formed, the next sequential entry out of the sender's transmit table **1208** is used to populate the IP source, IP destination, and IP header extension field (e.g., discriminator field). It will be appreciated that the transmit table need not be created in advance but could instead be created on-the-fly by executing the algorithm when each packet is formed.

At the receiving node **1202**, the same IP hop algorithm **1222**X is maintained and used to generate a receive table **1222** that lists valid triplets of source IP address, destination IP address, and discriminator field. This is shown by virtue of the first five entries of transmit table **1208** matching the second five entries of receive table **1222**. (The tables may be slightly offset at any particular time due to lost packets, misordered packets, or transmission delays). Additionally, node **1202** maintains a receive window **W3** that represents a list of valid IP source, IP destination, and discriminator fields that will be accepted when received as part of an incoming IP packet. As packets are received, window **W3** slides down the list of valid entries, such that the possible valid entries change over time. Two packets that arrive out of order but are nevertheless matched to entries within window **W3** will be accepted; those falling outside of window **W3** will be rejected as invalid. The length of window **W3** can be adjusted as necessary to reflect network delays or other factors.

Node **1202** maintains a similar transmit table **1221** for creating IP packets and frames destined for node **1201** using a potentially different hopping algorithm **1221**X, and node **1201** maintains a matching receive table **1209** using the same algorithm **1209**X. As node **1202** transmits packets to node **1201** using seemingly random IP source, IP destination, and/or discriminator fields, node **1201** matches the incoming packet values to those falling within window **W1** maintained in its receive table. In effect, transmit table **1208** of node **1201** is synchronized (i.e., entries are selected in the same order) to receive table **1222** of receiving node **1202**. Similarly, transmit table **1221** of node **1202** is synchronized to receive table **1209** of node **1201**. It will be appreciated that although a common algorithm is shown for the source, destination and discriminator fields in FIG. **12**A (using, e.g., a different seed for each of the three fields), an entirely different algorithm could in fact be used to establish values for each of these fields. It will also be appreciated that one or two of the fields can be "hopped" rather than all three as illustrated.

In accordance with another aspect of the invention, hardware or "MAC" addresses are hopped instead of or in addition to IP addresses and/or the discriminator field in order to improve security in a local area or broadcast-type network. To that end, node **1201** further maintains a transmit table **1210** using a transmit algorithm **1210**X to generate source and destination hardware addresses that are inserted into frame headers (e.g., fields **1101**A and **1101**B in FIG. **11**) that are synchronized to a corresponding receive table **1224** at node **1202**. Similarly, node **1202** maintains a different transmit table **1223** containing source and destination hardware addresses that is synchronized with a corresponding receive table **1211** at node **1201**. In this manner, outgoing hardware frames appear to be originating from and going to completely random nodes on the network, even though each recipient can determine whether a given packet is intended for it or not. It will be appreciated that the hardware hopping feature can be implemented at a different level in the communications protocol than the IP hopping feature (e.g., in a card driver or in a hardware card itself to improve performance).

FIG. **12**B shows three different embodiments or modes that can be employed using the aforementioned principles. In a first mode referred to as "promiscuous" mode, a

common hardware address (e.g., a fixed address for source and another for destination) or else a completely random hardware address is used by all nodes on the network, such that a particular packet cannot be attributed to any one node. Each node must initially accept all packets containing the common (or random) hardware address and inspect the IP addresses or discriminator field to determine whether the packet is intended for that node. In this regard, either the IP addresses or the discriminator field or both can be varied in accordance with an algorithm as described above. As explained previously, this may increase each node's overhead since additional processing is involved to determine whether a given packet has valid source and destination hardware addresses.

In a second mode referred to as "promiscuous per VPN" mode, a small set of fixed hardware addresses are used, with a fixed source/destination hardware address used for all nodes communicating over a virtual private network. For example, if there are six nodes on an Ethernet, and the network is to be split up into two private virtual networks such that nodes on one VPN can communicate with only the other two nodes on its own VPN, then two sets of hardware addresses could be used: one set for the first VPN and a second set for the second VPN. This would reduce the amount of overhead involved in checking for valid frames since only packets arriving from the designated VPN would need to be checked. IP addresses and one or more discriminator fields could still be hopped as before for secure communication within the VPN. Of course, this solution compromises the anonymity of the VPNs (i.e., an outsider can easily tell what traffic belongs in which VPN, though he cannot correlate it to a specific machine/person). It also requires the use of a discriminator field to mitigate the vulnerability to certain types of DoS attacks. (For example, without the discriminator field, an attacker on the LAN could stream frames containing the MAC addresses being used by the VPN; rejecting those frames could lead to excessive processing overhead. The discriminator field would provide a low-overhead means of rejecting the false packets.)

In a third mode referred to as "hardware hopping" mode, hardware addresses are varied as illustrated in FIG. **12**A, such that hardware source and destination addresses are changed constantly in order to provide non-attributable addressing. Variations on these embodiments are of course possible, and the invention is not intended to be limited in any respect by these illustrative examples.

B. Extending the Address Space

Address hopping provides security and privacy. However, the level of protection is limited by the number of addresses in the blocks being hopped. A hopblock denotes a field or fields modulated on a packet-wise basis for the purpose of providing a VPN. For instance, if two nodes communicate with IP address hopping using hopblocks of 4 addresses (2 bits) each, there would be 16 possible address-pair combinations. A window of size 16 would result in most address pairs being accepted as valid most of the time. This limitation can be overcome by using a discriminator field in addition to or instead of the hopped address fields. The discriminator field would be hopped in exactly the same fashion as the address fields and it would be used to determine whether a packet should be processed by a receiver.

Suppose that two clients, each using four-bit hopblocks, would like the same level of protection afforded to clients communicating via IP hopping between two A blocks (24 address bits eligible for hopping). A discriminator field of 20 bits, used in conjunction with the 4 address bits eligible for hopping in the IP address field, provides this level of protection. A 24-bit discriminator field would provide a similar level of protection if the address fields were not hopped or ignored. Using a discriminator field offers the following advantages: (1) an arbitrarily high level of protection can be provided, and (2) address hopping is unnecessary to provide protection. This may be important in environments where address hopping would cause routing problems.

C. Synchronization Techniques

It is generally assumed that once a sending node and receiving node have exchanged algorithms and seeds (or similar information sufficient to generate quasi-random source and destination tables), subsequent communication between the two nodes will proceed smoothly. Realistically, however, two nodes may lose synchronization due to network delays or outages, or other problems. Consequently, it is desirable to provide means for re-establishing synchronization between nodes in a network that have lost synchronization.

One possible technique is to require that each node provide an acknowledgment upon successful receipt of each packet and, if no acknowledgment is received within a certain period of time, to re-send the unacknowledged packet. This approach, however, drives up overhead costs and may be prohibitive in high-throughput environments such as streaming video or audio, for example.

A different approach is to employ an automatic synchronizing technique that will be referred to herein as "self-synchronization." In this approach, synchronization information is embedded into each packet, thereby enabling the receiver to re-synchronize itself upon receipt of a single packet if it determines that is has lost synchronization with the sender. (If communications are already in progress, and the receiver determines that it is still in sync with the sender, then there is no need to re-synchronize.) A receiver could detect that it was out of synchronization by, for example, employing a "dead-man" timer that expires after a certain period of time, wherein the timer is reset with each valid packet. A time stamp could be hashed into the public sync field (see below) to preclude packet-retry attacks.

In one embodiment, a "sync field" is added to the header of each packet sent out by the sender. This sync field could appear in the clear or as part of an encrypted portion of the packet. Assuming that a sender and receiver have selected a random-number generator (RNG) and seed value, this combination of RNG and seed can be used to generate a random-number sequence (RNS). The RNS is then used to generate a sequence of source/destination IP pairs (and, if desired, discriminator fields and hardware source and destination addresses), as described above. It is not necessary, however, to generate the entire sequence (or the first N-1 values) in order to generate the Nth random number in the sequence; if the sequence index N is known, the random value corresponding to that index can be directly generated (see below). Different RNGs (and seeds) with different fundamental periods could be used to generate the source and destination IP sequences, but the basic concepts would still apply. For the sake of simplicity, the following discussion will assume that IP source and destination address pairs (only) are hopped using a single RNG sequencing mechanism.

In accordance with a "self-synchronization" feature, a sync field in each packet header provides an index (i.e., a sequence number) into the RNS that is being used to generate IP pairs. Plugging this index into the RNG that is being used to generate the RNS yields a specific random number value, which in turn yields a specific IP pair. That is, an IP pair can be generated directly from knowledge of the RNG, seed, and index number; it is not necessary, in this scheme, to generate the entire sequence of random numbers that precede the sequence value associated with the index number provided.

Since the communicants have presumably previously exchanged RNGs and seeds, the only new information that must be provided in order to generate an IP pair is the sequence number. If this number is provided by the sender in the packet header, then the receiver need only plug this number into the RNG in order to generate an IP pair—and thus verify that the IP pair appearing in the header of the packet is valid. In this scheme, if the sender and receiver lose synchronization, the receiver can immediately re-synchronize upon receipt of a single packet by simply comparing the IP pair in the packet header to the IP pair generated from the index number. Thus, synchronized communications can be resumed upon receipt of a single packet, making this scheme ideal for multicast communications. Taken to the extreme, it could obviate the need for synchronization tables entirely; that is, the sender and receiver could simply rely on the index number in the sync field to validate the IP pair on each packet, and thereby eliminate the tables entirely.

The aforementioned scheme may have some inherent security issues associated with it—namely, the placement of the sync field. If the field is placed in the outer header, then an interloper could observe the values of the field and their relationship to the IP stream. This could potentially compromise the algorithm that is being used to generate the IP-address sequence, which would compromise the security of the communications. If, however, the value is placed in the inner header, then the sender must decrypt the inner header before it can extract the sync value and validate the IP pair; this opens up the receiver to certain types of denial-of-service (DoS) attacks, such as packet replay. That is, if the receiver must decrypt a packet before it can validate the IP pair, then it could potentially be forced to expend a significant amount of processing on decryption if an attacker simply retransmits previously valid packets. Other attack methodologies are possible in this scenario.

A possible compromise between algorithm security and processing speed is to split up the sync value between an inner (encrypted) and outer (unencrypted) header. That is, if the sync value is sufficiently long, it could potentially be split into a rapidly-changing part that can be viewed in the clear, and a fixed (or very slowly changing) part that must be protected. The part that can be viewed in the clear will be called the "public sync" portion and the part that must be protected will be called the "private sync" portion.

Both the public sync and private sync portions are needed to generate the complete sync value. The private portion, however, can be selected such that it is fixed or will change only occasionally. Thus, the private sync value can be stored by the recipient, thereby obviating the need to decrypt the header in order to retrieve it. If the sender and receiver have previously agreed upon the frequency with which the private part of the sync will change, then the receiver can selectively decrypt a single header in order to extract the new private sync if the communications gap that has led to lost synchronization has exceeded the lifetime of the previous private sync. This should not represent a burdensome amount of decryption, and thus should not open up the receiver to denial-of-service attack simply based on the need to occasionally decrypt a single header.

One implementation of this is to use a hashing function with a one-to-one mapping to generate the private and public sync portions from the sync value. This implementation is shown in FIG. **13**, where (for example) a first ISP **1302** is the sender and a second ISP **1303** is the receiver. (Other alternatives are possible from FIG. **13**.) A transmitted packet comprises a public or "outer" header **1305** that is not encrypted, and a private or "inner" header **1306** that is encrypted using for example a link key. Outer header **1305** includes a public sync portion while inner header **1306** contains the private sync portion. A receiving node decrypts the inner header using a decryption function **1307** in order to extract the private sync portion. This step is necessary only if the lifetime of the currently buffered private sync has expired. (If the currently-buffered private sync is still valid, then it is simply extracted from memory and "added" (which could be an inverse hash) to the public sync, as shown in step **1308**.) The public and decrypted private sync portions are combined in function **1308** in order to generate the combined sync **1309**. The combined sync (**1309**) is then fed into the RNG (**1310**) and compared to the IP address pair (**1311**) to validate or reject the packet.

An important consideration in this architecture is the concept of "future" and "past" where the public sync values are concerned. Though the sync values, themselves, should be random to prevent spoofing attacks, it may be important that the receiver be able to quickly identify a sync value that has already been sent—even if the packet containing that sync value was never actually received by the receiver. One solution is to hash a time stamp or sequence number into the public sync portion, which could be quickly extracted, checked, and discarded, thereby validating the public sync portion itself.

In one embodiment, packets can be checked by comparing the source/destination IP pair generated by the sync field with the pair appearing in the packet header. If (1) they match, (2) the time stamp is valid, and (3) the dead-man timer has expired, then re-synchronization occurs; otherwise, the packet is rejected. If enough processing power is available, the dead-man timer and synchronization tables can be avoided altogether, and the receiver would simply resynchronize (e.g., validate) on every packet.

The foregoing scheme may require large-integer (e.g., 160-bit) math, which may affect its implementation. Without such large-integer registers, processing throughput would be affected, thus potentially affecting security from a denial-of-service standpoint. Nevertheless, as large-integer math processing features become more prevalent, the costs of implementing such a feature will be reduced.

D. Other Synchronization Schemes

As explained above, if W or more consecutive packets are lost between a transmitter and receiver in a VPN (where W is the window size), the receiver's window will not have been updated and the transmitter will be transmitting packets not in the receiver's window. The sender and receiver will not recover synchronization until perhaps the random pairs in the window are repeated by chance. Therefore, there is a need to keep a transmitter and receiver in synchronization whenever possible and to re-establish synchronization whenever it is lost.

A "checkpoint" scheme can be used to regain synchronization between a sender and a receiver that have fallen out

of synchronization. In this scheme, a checkpoint message comprising a random IP address pair is used for communicating synchronization information. In one embodiment, two messages are used to communicate synchronization information between a sender and a recipient:

1. SYNC_REQ is a message used by the sender to indicate that it wants to synchronize; and
2. SYNC_ACK is a message used by the receiver to inform the transmitter that it has been synchronized.

According to one variation of this approach, both the transmitter and receiver maintain three checkpoints (see FIG. 14):

1. In the transmitter, ckpt_o ("checkpoint old") is the IP pair that was used to re-send the last SYNC_REQ packet to the receiver. In the receiver, ckpt_o ("checkpoint old") is the IP pair that receives repeated SYNC_REQ packets from the transmitter.
2. In the transmitter, ckpt_n ("checkpoint new") is the IP pair that will be used to send the next SYNC_REQ packet to the receiver. In the receiver, ckpt_n ("checkpoint new") is the IP pair that receives a new SYNC_REQ packet from the transmitter and which causes the receiver's window to be re-aligned, ckpt_o set to ckpt_n, a new ckpt_n to be generated and a new ckpt_r to be generated.
3. In the transmitter, ckpt_r is the IP pair that will be used to send the next SYNC_ACK packet to the receiver. In the receiver, ckpt_r is the IP pair that receives a new SYNC_ACK packet from the transmitter and which causes a new ckpt_n to be generated. Since SYNC_ACK is transmitted from the receiver ISP to the sender ISP, the transmitter ckpt_r refers to the ckpt_r of the receiver and the receiver ckpt_r refers to the ckpt_r of the transmitter (see FIG. 14).

When a transmitter initiates synchronization, the IP pair it will use to transmit the next data packet is set to a predetermined value and when a receiver first receives a SYNC_REQ, the receiver window is updated to be centered on the transmitter's next IP pair. This is the primary mechanism for checkpoint synchronization.

Synchronization can be initiated by a packet counter (e.g., after every N packets transmitted, initiate a synchronization) or by a timer (every S seconds, initiate a synchronization) or a combination of both. See FIG. 15. From the transmitter's perspective, this technique operates as follows: (1) Each transmitter periodically transmits a "sync request" message to the receiver to make sure that it is in sync. (2) If the receiver is still in sync, it sends back a "sync ack" message. (If this works, no further action is necessary). (3) If no "sync ack" has been received within a period of time, the transmitter retransmits the sync request again. If the transmitter reaches the next checkpoint without receiving a "sync ack" response, then synchronization is broken, and the transmitter should stop transmitting. The transmitter will continue to send sync_reqs until it receives a sync_ack, at which point transmission is reestablished.

From the receiver's perspective, the scheme operates as follows: (1) when it receives a "sync request" request from the transmitter, it advances its window to the next checkpoint position (even skipping pairs if necessary), and sends a "sync ack" message to the transmitter. If sync was never lost, then the "jump ahead" really just advances to the next available pair of addresses in the table (i.e., normal advancement).

If an interloper intercepts the "sync request" messages and tries to interfere with communication by sending new ones, it will be ignored if the synchronization has been established or it will actually help to re-establish synchronization.

A window is realigned whenever a re-synchronization occurs. This realignment entails updating the receiver's window to straddle the address pairs used by the packet transmitted immediately after the transmission of the SYNC_REQ packet. Normally, the transmitter and receiver are in synchronization with one another. However, when network events occur, the receiver's window may have to be advanced by many steps during resynchronization. In this case, it is desirable to move the window ahead without having to step through the intervening random numbers sequentially. (This feature is also desirable for the auto-sync approach discussed above).

E. Random Number Generator with a Jump-Ahead Capability

An attractive method for generating randomly hopped addresses is to use identical random number generators in the transmitter and receiver and advance them as packets are transmitted and received. There are many random number generation algorithms that could be used. Each one has strengths and weaknesses for address hopping applications.

Linear congruential random number generators (LCRs) are fast, simple and well characterized random number generators that can be made to jump ahead n steps efficiently. An LCR generates random numbers $X_1, X_2, X_3 \ldots X_k$ starting with seed X_0 using a recurrence

$$X_i=(a\,X_{i-1}+b) \bmod c, \tag{1}$$

where a, b and c define a particular LCR. Another expression for X_n,

$$X_i=((a^i(X_0+b)-b)/(a-1)) \bmod c \tag{2}$$

enables the jump-ahead capability. The factor a^i can grow very large even for modest i if left unfettered. Therefore some special properties of the modulo operation can be used to control the size and processing time required to compute (2). (2) can be rewritten as:

$$X_i=(a^i(X_0(c-1)+b)-b)/(a-1) \bmod c. \tag{3}$$

It can be shown that:

$$(a^i(X_0(a-1)+b)-b)/(a-1) \bmod c=((a^i \bmod((a-1)c))(X_0(a-1)+b)-b)/(a-1)) \bmod c \tag{4}$$

$(X_0(a-1)+b)$ can be stored as $(X_0(a-1)+b) \bmod c$, b as b mod c and compute $a^i \bmod((a-1)c)$ (this requires O(log(i)) steps).

A practical implementation of this algorithm would jump a fixed distance, n, between synchronizations; this is tantamount to synchronizing every n packets. The window would commence n IP pairs from the start of the previous window. Using X_j^m, the random number at the jth checkpoint, as X_0 and n as i, a node can store $a^n \bmod((a-1)c)$ once per LCR and set

$$X_{j+1}^m=X_{n(j+1)}=((a^n \bmod((a-1)c))(X_j^m(a-1)+b)-b)/(a-1)) \bmod c, \tag{5}$$

to generate the random number for the $j+1^{th}$ synchronization. Using this construction, a node could jump ahead an arbitrary (but fixed) distance between synchronizations in a constant amount of time (independent of n).

Pseudo-random number generators, in general, and LCRs, in particular, will eventually repeat their cycles. This repetition may present vulnerability in the IP hopping scheme.

An adversary would simply have to wait for a repeat to predict future sequences. One way of coping with this vulnerability is to create a random number generator with a known long cycle. A random sequence can be replaced by a new random number generator before it repeats. LCRs can be constructed with known long cycles. This is not currently true of many random number generators.

Random number generators can be cryptographically insecure. An adversary can derive the RNG parameters by examining the output or part of the output. This is true of LCGs. This vulnerability can be mitigated by incorporating an encryptor, designed to scramble the output as part of the random number generator. The random number generator prevents an adversary from mounting an attack—e.g., a known plaintext attack—against the encryptor.

F. Random Number Generator Example

Consider a RNG where a 31, b 4 and c 15. For this case equation (1) becomes:

$$X_i=(31\,X_{i-1}+4) \bmod 15. \quad (6)$$

If one sets $X_0=1$, equation (6) will produce the sequence 1, 5, 9, 13, 2, 6, 10, 14, 3, 7, 11, 0, 4, 8, 12. This sequence will repeat indefinitely. For a jump ahead of 3 numbers in this sequence $a''=31^3=29791$, $c^*(a-1)=15^*30=450$ and $a'' \bmod((a-1)c)=31^3 \bmod(15^*30)=29791 \bmod(450)=91$. Equation (5) becomes:

$$((91(X_i30+4)-4)/30) \bmod 15 \quad (7).$$

Table 1 shows the jump ahead calculations from (7). The calculations start at 5 and jump ahead 3.

TABLE 1

I	X_i	(X_i30+4)	$91\,(X_i30+4)-4$	$((91\,(X_i30+4)-4)/30$	X_{i+3}
1	5	154	14010	467	2
4	2	64	5820	194	14
7	14	424	38580	1286	11
10	11	334	30390	1013	8
13	8	244	22200	740	5

G. Fast Packet Filter

Address hopping VPNs must rapidly determine whether a packet has a valid header and thus requires further processing, or has an invalid header (a hostile packet) and should be immediately rejected. Such rapid determinations will be referred to as "fast packet filtering." This capability protects the VPN from attacks by an adversary who streams hostile packets at the receiver at a high rate of speed in the hope of saturating the receiver's processor (a so-called "denial of service" attack). Fast packet filtering is an important feature for implementing VPNs on shared media such as Ethernet.

Assuming that all participants in a VPN share an unassigned "A" block of addresses, one possibility is to use an experimental "A" block that will never be assigned to any machine that is not address hopping on the shared medium. "A" blocks have a 24 bits of address that can be hopped as opposed to the 8 bits in "C" blocks. In this case a hopblock will be the "A" block. The use of the experimental "A" block is a likely option on an Ethernet because:

1. The addresses have no validity outside of the Ethernet and will not be routed out to a valid outside destination by a gateway.
2. There are 2^{24} (~16 million) addresses that can be hopped within each "A" block. This yields >280 trillion possible address pairs making it very unlikely that an adversary would guess a valid address. It also provides acceptably low probability of collision between separate VPNs (all VPNs on a shared medium independently generate random address pairs from the same "A" block).
3. The packets will not be received by someone on the Ethernet who is not on a VPN (unless the machine is in promiscuous mode) minimizing impact on non-VPN computers.

The Ethernet example will be used to describe one implementation of fast packet filtering. The ideal algorithm would quickly examine a packet header, determine whether the packet is hostile, and reject any hostile packets or determine which active IP pair the packet header matches. The problem is a classical associative memory problem. A variety of techniques have been developed to solve this problem (hashing, B-trees etc). Each of these approaches has its strengths and weaknesses. For instance, hash tables can be made to operate quite fast in a statistical sense, but can occasionally degenerate into a much slower algorithm. This slowness can persist for a period of time. Since there is a need to discard hostile packets quickly at all times, hashing would be unacceptable.

H. Presence Vector Algorithm

A presence vector is a bit vector of length 2^n that can be indexed by n-bit numbers (each ranging from 0 to 2^n-1). One can indicate the presence of k n-bit numbers (not necessarily unique), by setting the bits in the presence vector indexed by each number to 1. Otherwise, the bits in the presence vector are 0. An n-bit number, x, is one of the k numbers if and only if the xth bit of the presence vector is 1. A fast packet filter can be implemented by indexing the presence vector and looking for a 1, which will be referred to as the "test."

For example, suppose one wanted to represent the number 135 using a presence vector. The 135th bit of the vector would be set. Consequently, one could very quickly determine whether an address of 135 was valid by checking only one bit: the 135th bit. The presence vectors could be created in advance corresponding to the table entries for the IP addresses. In effect, the incoming addresses can be used as indices into a long vector, making comparisons very fast. As each RNG generates a new address, the presence vector is updated to reflect the information. As the window moves, the presence vector is updated to zero out addresses that are no longer valid.

There is a trade-off between efficiency of the test and the amount of memory required for storing the presence vector(s). For instance, if one were to use the 48 bits of hopping addresses as an index, the presence vector would have to be 35 terabytes. Clearly, this is too large for practical purposes. Instead, the 48 bits can be divided into several smaller fields. For instance, one could subdivide the 48 bits into four 12-bit fields (see FIG. 16). This reduces the storage requirement to 2048 bytes at the expense of occasionally having to process a hostile packet. In effect, instead of one long presence vector, the decomposed address portions must match all four shorter presence vectors before further processing is allowed. (If the first part of the address portion doesn't match the first presence vector, there is no need to check the remaining three presence vectors).

A presence vector will have a 1 in the yth bit if and only if one or more addresses with a corresponding field of y are

Petitioner Apple Inc. - Exhibit 1002, p. 558

active. An address is active only if each presence vector indexed by the appropriate sub-field of the address is 1.

Consider a window of 32 active addresses and 3 checkpoints. A hostile packet will be rejected by the indexing of one presence vector more than 99% of the time. A hostile packet will be rejected by the indexing of all 4 presence vectors more than 99.9999995% of the time. On average, hostile packets will be rejected in less than 1.02 presence vector index operations.

The small percentage of hostile packets that pass the fast packet filter will be rejected when matching pairs are not found in the active window or are active checkpoints. Hostile packets that serendipitously match a header will be rejected when the VPN software attempts to decrypt the header. However, these cases will be extremely rare. There are many other ways this method can be configured to arbitrate the space/speed tradeoffs.

1. Further Synchronization Enhancements

A slightly modified form of the synchronization techniques described above can be employed. The basic principles of the previously described checkpoint synchronization scheme remain unchanged. The actions resulting from the reception of the checkpoints are, however, slightly different. In this variation, the receiver will maintain between OoO ("Out of Order") and 2×WINDOW_SIZE+OoO active addresses ($1 \leqq OoO \leqq WINDOW\_SIZE$ and $WINDOW\_SIZE \geqq 1$). OoO and WINDOW_SIZE are engineerable parameters, where OoO is the minimum number of addresses needed to accommodate lost packets due to events in the network or out of order arrivals and WINDOW_SIZE is the number of packets transmitted before a SYNC_REQ is issued. FIG. **17** depicts a storage array for a receiver's active addresses.

The receiver starts with the first 2×WINDOW_SIZE addresses loaded and active (ready to receive data). As packets are received, the corresponding entries are marked as "used" and are no longer eligible to receive packets. The transmitter maintains a packet counter, initially set to 0, containing the number of data packets transmitted since the last initial transmission of a SYNC_REQ for which SYNC_ACK has been received. When the transmitter packet counter equals WINDOW_SIZE, the transmitter generates a SYNC_REQ and does its initial transmission. When the receiver receives a SYNC_REQ corresponding to its current CKPT_N, it generates the next WINDOW_SIZE addresses and starts loading them in order starting at the first location after the last active address wrapping around to the beginning of the array after the end of the array has been reached. The receiver's array might look like FIG. **18** when a SYNC_REQ has been received. In this case a couple of packets have been either lost or will be received out of order when the SYNC_REQ is received.

FIG. **19** shows the receiver's array after the new addresses have been generated. If the transmitter does not receive a SYNC_ACK, it will re-issue the SYNC_REQ at regular intervals. When the transmitter receives a SYNC_ACK, the packet counter is decremented by WINDOW_SIZE. If the packet counter reaches 2×WINDOW_SIZE−OoO then the transmitter ceases sending data packets until the appropriate SYNC_ACK is finally received. The transmitter then resumes sending data packets. Future behavior is essentially a repetition of this initial cycle. The advantages of this approach are:

1. There is no need for an efficient jump ahead in the random number generator,
2. No packet is ever transmitted that does not have a corresponding entry in the receiver side
3. No timer based re-synchronization is necessary. This is a consequence of 2.
4. The receiver will always have the ability to accept data messages transmitted within OoO messages of the most recently transmitted message.

J. Distributed Transmission Path Variant

Another embodiment incorporating various inventive principles is shown in FIG. **20**. In this embodiment, a message transmission system includes a first computer **2001** in communication with a second computer **2002** through a network **2011** of intermediary computers. In one variant of this embodiment, the network includes two edge routers **2003** and **2004** each of which is linked to a plurality of Internet Service Providers (ISPs) **2005** through **2010**. Each ISP is coupled to a plurality of other ISPs in an arrangement as shown in FIG. **20**, which is a representative configuration only and is not intended to be limiting. Each connection between ISPs is labeled in FIG. **20** to indicate a specific physical transmission path (e.g., AD is a physical path that links ISP A (element **2005**) to ISP D (element **2008**)). Packets arriving at each edge router are selectively transmitted to one of the ISPs to which the router is attached on the basis of a randomly or quasi-randomly selected basis.

As shown in FIG. **21**, computer **2001** or edge router **2003** incorporates a plurality of link transmission tables **2100** that identify, for each potential transmission path through the network, valid sets of IP addresses that can be used to transmit the packet. For example, AD table **2101** contains a plurality of IP source/destination pairs that are randomly or quasi-randomly generated. When a packet is to be transmitted from first computer **2001** to second computer **2002**, one of the link tables is randomly (or quasi-randomly) selected, and the next valid source/destination address pair from that table is used to transmit the packet through the network. If path AD is randomly selected, for example, the next source/destination IP address pair (which is pre-determined to transmit between ISP A (element **2005**) and ISP B (element **2008**)) is used to transmit the packet. If one of the transmission paths becomes degraded or inoperative, that link table can be set to a "down" condition as shown in table **2105**, thus preventing addresses from being selected from that table. Other transmission paths would be unaffected by this broken link.

3. Continuation-in-Part Improvements

The following describes various improvements and features that can be applied to the embodiments described above. The improvements include: (1) a load balancer that distributes packets across different transmission paths according to transmission path quality; (2) a DNS proxy server that transparently creates a virtual private network in response to a domain name inquiry; (3) a large-to-small link bandwidth management feature that prevents denial-of-service attacks at system chokepoints; (4) a traffic limiter that regulates incoming packets by limiting the rate at which a transmitter can be synchronized with a receiver; and (5) a signaling synchronizer that allows a large number of nodes to communicate with a central node by partitioning the communication function between two separate entities. Each is discussed separately below.

Petitioner Apple Inc. - Exhibit 1002, p. 559

A. Load Balancer

Various embodiments described above include a system in which a transmitting node and a receiving node are coupled through a plurality of transmission paths, and wherein successive packets are distributed quasi-randomly over the plurality of paths. See, for example, FIGS. **20** and **21** and accompanying description. The improvement extends this basic concept to encompass distributing packets across different paths in such a manner that the loads on the paths are generally balanced according to transmission link quality.

In one embodiment, a system includes a transmitting node and a receiving node that are linked via a plurality of transmission paths having potentially varying transmission quality. Successive packets are transmitted over the paths based on a weight value distribution function for each path. The rate that packets will be transmitted over a given path can be different for each path. The relative "health" of each transmission path is monitored in order to identify paths that have become degraded. In one embodiment, the health of each path is monitored in the transmitter by comparing the number of packets transmitted to the number of packet acknowledgements received. Each transmission path may comprise a physically separate path (e.g., via dial-up phone line, computer network, router, bridge, or the like), or may comprise logically separate paths contained within a broadband communication medium (e.g., separate channels in an FDM, TDM, CDMA, or other type of modulated or unmodulated transmission link).

When the transmission quality of a path falls below a predetermined threshold and there are other paths that can transmit packets, the transmitter changes the weight value used for that path, making it less likely that a given packet will be transmitted over that path. The weight will preferably be set no lower than a minimum value that keeps nominal traffic on the path. The weights of the other available paths are altered to compensate for the change in the affected path. When the quality of a path degrades to where the transmitter is turned off by the synchronization function (i.e., no packets are arriving at the destination), the weight is set to zero. If all transmitters are turned off, no packets are sent.

Conventional TCP/IP protocols include a "throttling" feature that reduces the transmission rate of packets when it is determined that delays or errors are occurring in transmission. In this respect, timers are sometimes used to determine whether packets have been received. These conventional techniques for limiting transmission of packets, however, do not involve multiple transmission paths between two nodes wherein transmission across a particular path relative to the others is changed based on link quality.

According to certain embodiments, in order to damp oscillations that might otherwise occur if weight distributions are changed drastically (e.g., according to a step function), a linear or an exponential decay formula can be applied to gradually decrease the weight value over time that a degrading path will be used. Similarly, if the health of a degraded path improves, the weight value for that path is gradually increased.

Transmission link health can be evaluated by comparing the number of packets that are acknowledged within the transmission window (see embodiments discussed above) to the number of packets transmitted within that window and by the state of the transmitter (i.e., on or off). In other words, rather than accumulating general transmission statistics over time for a path, one specific implementation uses the "windowing" concepts described above to evaluate transmission path health.

The same scheme can be used to shift virtual circuit paths from an "unhealthy" path to a "healthy" one, and to select a path for a new virtual circuit.

FIG. **22A** shows a flowchart for adjusting weight values associated with a plurality of transmission links. It is assumed that software executing in one or more computer nodes executes the steps shown in FIG. **22A**. It is also assumed that the software can be stored on a computer-readable medium such as a magnetic or optical disk for execution by a computer.

Beginning in step **2201**, the transmission quality of a given transmission path is measured. As described above, this measurement can be based on a comparison between the number of packets transmitted over a particular link to the number of packet acknowledgements received over the link (e.g., per unit time, or in absolute terms). Alternatively, the quality can be evaluated by comparing the number of packets that are acknowledged within the transmission window to the number of packets that were transmitted within that window. In yet another variation, the number of missed synchronization messages can be used to indicate link quality. Many other variations are of course possible.

In step **2202**, a check is made to determine whether more than one transmitter (e.g., transmission path) is turned on. If not, the process is terminated and resumes at step **2201**.

In step **2203**, the link quality is compared to a given threshold (e.g., 50%, or any arbitrary number). If the quality falls below the threshold, then in step **2207** a check is made to determine whether the weight is above a minimum level (e.g., 1%). If not, then in step **2209** the weight is set to the minimum level and processing resumes at step **2201**. If the weight is above the minimum level, then in step **2208** the weight is gradually decreased for the path, then in step **2206** the weights for the remaining paths are adjusted accordingly to compensate (e.g., they are increased).

If in step **2203** the quality of the path was greater than or equal to the threshold, then in step **2204** a check is made to determine whether the weight is less than a steady-state value for that path. If so, then in step **2205** the weight is increased toward the steady-state value, and in step **2206** the weights for the remaining paths are adjusted accordingly to compensate (e.g., they are decreased). If in step **2204** the weight is not less than the steady-state value, then processing resumes at step **2201** without adjusting the weights.

The weights can be adjusted incrementally according to various functions, preferably by changing the value gradually. In one embodiment, a linearly decreasing function is used to adjust the weights; according to another embodiment, an exponential decay function is used. Gradually changing the weights helps to damp oscillators that might otherwise occur if the probabilities were abruptly.

Although not explicitly shown in FIG. **22A** the process can be performed only periodically (e.g., according to a time schedule), or it can be continuously run, such as in a background mode of operation. In one embodiment, the combined weights of all potential paths should add up to unity (e.g., when the weighting for one path is decreased, the corresponding weights that the other paths will be selected will increase).

Adjustments to weight values for other paths can be prorated. For example, a decrease of 10% in weight value for one path could result in an evenly distributed increase in the weights for the remaining paths. Alternatively, weightings could be adjusted according to a weighted formula as

desired (e.g., favoring healthy paths over less healthy paths). In yet another variation, the difference in weight value can be amortized over the remaining links in a manner that is proportional to their traffic weighting.

FIG. **22B** shows steps that can be executed to shut down transmission links where a transmitter turns off. In step **2210**, a transmitter shut-down event occurs. In step **2211**, a test is made to determine whether at least one transmitter is still turned on. If not, then in step **2215** all packets are dropped until a transmitter turns on. If in step **2211** at least one transmitter is turned on, then in step **2212** the weight for the path is set to zero, and the weights for the remaining paths are adjusted accordingly.

FIG. **23** shows a computer node **2301** employing various principles of the above-described embodiments. It is assumed that two computer nodes of the type shown in FIG. **23** communicate over a plurality of separate physical transmission paths. As shown in FIG. **23**, four transmission paths X1 through X4 are defined for communicating between the two nodes. Each node includes a packet transmitter **2302** that operates in accordance with a transmit table **2308** as described above. (The packet transmitter could also operate without using the IP-hopping features described above, but the following description assumes that some form of hopping is employed in conjunction with the path selection mechanism.). The computer node also includes a packet receiver **2303** that operates in accordance with a receive table **2309**, including a moving window W that moves as valid packets are received. Invalid packets having source and destination addresses that do not fall within window W are rejected.

As each packet is readied for transmission, source and destination IP addresses (or other discriminator values) are selected from transmit table **2308** according to any of the various algorithms described above, and packets containing these source/destination address pairs, which correspond to the node to which the four transmission paths are linked, are generated to a transmission path switch **2307**. Switch **2307**, which can comprise a software function, selects from one of the available transmission paths according to a weight distribution table **2306**. For example, if the weight for path X1 is 0.2, then every fifth packet will be transmitted on path X1. A similar regime holds true for the other paths as shown. Initially, each link's weight value can be set such that it is proportional to its bandwidth, which will be referred to as its "steady-state" value.

Packet receiver **2303** generates an output to a link quality measurement function **2304** that operates as described above to determine the quality of each transmission path. (The input to packet receiver **2303** for receiving incoming packets is omitted for clarity). Link quality measurement function **2304** compares the link quality to a threshold for each transmission link and, if necessary, generates an output to weight adjustment function **2305**. If a weight adjustment is required, then the weights in table **2306** are adjusted accordingly, preferably according to a gradual (e.g., linearly or exponentially declining) function. In one embodiment, the weight values for all available paths are initially set to the same value, and only when paths degrade in quality are the weights changed to reflect differences.

Link quality measurement function **2304** can be made to operate as part of a synchronizer function as described above. That is, if resynchronization occurs and the receiver detects that synchronization has been lost (e.g., resulting in the synchronization window W being advanced out of sequence), that fact can be used to drive link quality measurement function **2304**. According to one embodiment, load balancing is performed using information garnered during the normal synchronization, augmented slightly to communicate link health from the receiver to the transmitter. The receiver maintains a count, MESS_R(W), of the messages received in synchronization window W. When it receives a synchronization request (SYNC_REQ) corresponding to the end of window W, the receiver includes counter MESS_R in the resulting synchronization acknowledgement (SYNC_ACK) sent back to the transmitter. This allows the transmitter to compare messages sent to messages received in order to asses the health of the link.

If synchronization is completely lost, weight adjustment function **2305** decreases the weight value on the affected path to zero. When synchronization is regained, the weight value for the affected path is gradually increased to its original value. Alternatively, link quality can be measured by evaluating the length of time required for the receiver to acknowledge a synchronization request. In one embodiment, separate transmit and receive tables are used for each transmission path.

When the transmitter receives a SYNC_ACK, the MESS_R is compared with the number of messages transmitted in a window (MESS_T). When the transmitter receives a SYNC_ACK, the traffic probabilities will be examined and adjusted if necessary. MESS_R is compared with the number of messages transmitted in a window (MESS_T). There are two possibilities:

1. If MESS_R is less than a threshold value, THRESH, then the link will be deemed to be unhealthy. If the transmitter was turned off, the transmitter is turned on and the weight P for that link will be set to a minimum value MIN. This will keep a trickle of traffic on the link for monitoring purposes until it recovers. If the transmitter was turned on, the weight P for that link will be set to:

$$P\alpha\times MIN+(1-\alpha)\times P \tag{1}$$

Equation 1 will exponentially damp the traffic weight value to MIN during sustained periods of degraded service.

2. If MESS_R for a link is greater than or equal to THRESH, the link will be deemed healthy. If the weight P for that link is greater than or equal to the steady state value S for that link, then P is left unaltered. If the weight P for that link is less than THRESH then P will be set to:

$$P'-\beta\times S+(1-\beta)\times P \tag{2}$$

where β is a parameter such that $0<=\beta<=1$ that determines the damping rate of P.

Equation 2 will increase the traffic weight to S during sustained periods of acceptable service in a damped exponential fashion.

A detailed example will now be provided with reference to FIG. **24**. As shown in FIG. **24**, a first computer **2401** communicates with a second computer **2402** through two routers **2403** and **2404**. Each router is coupled to the other router through three transmission links. As described above, these may be physically diverse links or logical links (including virtual private networks).

Suppose that a first link L1 can sustain a transmission bandwidth of 100 Mb/s and has a window size of 32; link L2 can sustain 75 Mb/s and has a window size of 24; and link L3 can sustain 25 Mb/s and has a window size of 8. The combined links can thus sustain 200 Mb/s. The steady state traffic weights are 0.5 for link L1; 0.375 for link L2, and 0.125 for link L3. MIN=1 Mb/s, THRESH=0.8 MESS_T for each link, α=0.75 and β=0.5. These traffic weights will remain stable until a link stops for synchronization or reports

a number of packets received less than its THRESH. Consider the following sequence of events:

1. Link L1 receives a SYNC_ACK containing a MESS_R of 24, indicating that only 75% of the MESS_T (32) messages transmitted in the last window were successfully received. Link 1 would be below THRESH (0.8). Consequently, link L1's traffic weight value would be reduced to 0.12825, while link L2's traffic weight value would be increased to 0.65812 and link L3's traffic weight value would be increased to 0.217938.

2. Link L2 and L3 remained healthy and link L1 stopped to synchronize. Then link L1's traffic weight value would be set to 0, link L2's traffic weight value would be set to 0.75, and link L33's traffic weight value would be set to 0.25.

3. Link L1 finally received a SYNC_ACK containing a MESS_R of 0 indicating that none of the MESS_T (32) messages transmitted in the last window were successfully received. Link L1 would be below THRESH. Link L1's traffic weight value would be increased to 0.005, link L2's traffic weight value would be decreased to 0.74625, and link L3's traffic weight value would be decreased to 0.24875.

4. Link L1 received a SYNC_ACK containing a MESS_R of 32 indicating that 100% of the MESS_T (32) messages transmitted in the last window were successfully received. Link L1 would be above THRESH. Link L1's traffic weight value would be increased to 0.2525, while link L2's traffic weight value would be decreased to 0.560625 and link L3's traffic weight value would be decreased to 0.186875.

5. Link L1 received a SYNC_ACK containing a MESS_R of 32 indicating that 100% of the MESS_T (32) messages transmitted in the last window were successfully received. Link L1 would be above THRESH. Link L1's traffic weight value would be increased to 0.37625; link L2's traffic weight value would be decreased to 0.4678125, and link L3's traffic weight value would be decreased to 0.1559375.

6. Link L1 remains healthy and the traffic probabilities approach their steady state traffic probabilities.

B. Use of a DNS Proxy to Transparently Create Virtual Private Networks

A second improvement concerns the automatic creation of a virtual private network (VPN) in response to a domain-name server look-up function.

Conventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host. For example, when a computer user types in the web name "Yahoo.com," the user's web browser transmits a request to a DNS, which converts the name into a four-part IP address that is returned to the user's browser and then used by the browser to contact the destination web site.

This conventional scheme is shown in FIG. **25**. A user's computer **2501** includes a client application **2504** (for example, a web browser) and an IP protocol stack **2505**. When the user enters the name of a destination host, a request DNS REQ is made (through IP protocol stack **2505**) to a DNS **2502** to look up the IP address associated with the name. The DNS returns the IP address DNS RESP to client application **2504**, which is then able to use the IP address to communicate with the host **2503** through separate transactions such as PAGE REQ and PAGE RESP.

In the conventional architecture shown in FIG. **25**, nefarious listeners on the Internet could intercept the DNS REQ and DNS RESP packets and thus learn what IP addresses the user was contacting. For example, if a user wanted to set up a secure communication path with a web site having the name "Target.com," when the user's browser contacted a DNS to find the IP address for that web site, the true IP address of that web site would be revealed over the Internet as part of the DNS inquiry. This would hamper anonymous communications on the Internet.

One conventional scheme that provides secure virtual private networks over the Internet provides the DNS server with the public keys of the machines that the DNS server has the addresses for. This allows hosts to retrieve automatically the public keys of a host that the host is to communicate with so that the host can set up a VPN without having the user enter the public key of the destination host. One implementation of this standard is presently being developed as part of the FreeS/WAN project(RFC 2535).

The conventional scheme suffers from certain drawbacks. For example, any user can perform a DNS request. Moreover, DNS requests resolve to the same value for all users.

According to certain aspects of the invention, a specialized DNS server traps DNS requests and, if the request is from a special type of user (e.g., one for which secure communication services are defined), the server does not return the true IP address of the target node, but instead automatically sets up a virtual private network between the target node and the user. The VPN is preferably implemented using the IP address "hopping" features of the basic invention described above, such that the true identity of the two nodes cannot be determined even if packets during the communication are intercepted. For DNS requests that are determined to not require secure services (e.g., an unregistered user), the DNS server transparently "passes through" the request to provide a normal look-up function and return the IP address of the target web server, provided that the requesting host has permissions to resolve unsecured sites. Different users who make an identical DNS request could be provided with different results.

FIG. **26** shows a system employing various principles summarized above. A user's computer **2601** includes a conventional client (e.g., a web browser) **2605** and an IP protocol stack **2606** that preferably operates in accordance with an IP hopping function **2607** as outlined above. A modified DNS server **2602** includes a conventional DNS server function **2609** and a DNS proxy **2610**. A gatekeeper server **2603** is interposed between the modified DNS server and a secure target site **2704**. An "unsecure" target site **2611** is also accessible via conventional IP protocols.

According to one embodiment, DNS proxy **2610** intercepts all DNS lookup functions from client **2605** and determines whether access to a secure site has been requested. If access to a secure site has been requested (as determined, for example, by a domain name extension, or by reference to an internal table of such sites), DNS proxy **2610** determines whether the user has sufficient security privileges to access the site. If so, DNS proxy **2610** transmits a message to gatekeeper **2603** requesting that a virtual private network be created between user computer **2601** and secure target site **2604**. In one embodiment, gatekeeper **2603** creates "hopblocks" to be used by computer **2601** and secure target site **2604** for secure communication. Then, gatekeeper **2603** communicates these to user computer **2601**. Thereafter, DNS proxy **2610** returns to user computer **2601** the resolved address passed to it by the gatekeeper (this address could be different from the actual target computer) **2604**, preferably using a secure administrative VPN. The address that is returned need not be the actual address of the destination computer.

Had the user requested lookup of a non-secure web site such as site **2611**, DNS proxy would merely pass through to

conventional DNS server **2609** the look-up request, which would be handled in a conventional manner, returning the IP address of non-secure web site **2611**. If the user had requested lookup of a secure web site but lacked credentials to create such a connection, DNS proxy **2610** would return a "host unknown" error to the user. In this manner, different users requesting access to the same DNS name could be provided with different look-up results.

Gatekeeper **2603** can be implemented on a separate computer (as shown in FIG. **26**) or as a function within modified DNS server **2602**. In general, it is anticipated that gatekeeper **2703** facilitates the allocation and exchange of information needed to communicate securely, such as using "hopped" IP addresses. Secure hosts such as site **2604** are assumed to be equipped with a secure communication function such as an IP hopping function **2608**.

It will be appreciated that the functions of DNS proxy **2610** and DNS server **2609** can be combined into a single server for convenience. Moreover, although element **2602** is shown as combining the functions of two servers, the two servers can be made to operate independently.

FIG. **27** shows steps that can be executed by DNS proxy server **2610** to handle requests for DNS look-up for secure hosts. In step **2701**, a DNS look-up request is received for a target host. In step **2702**, a check is made to determine whether access to a secure host was requested. If not, then in step **2703** the DNS request is passed to conventional DNS server **2609**, which looks up the IP address of the target site and returns it to the user's application for further processing.

In step **2702**, if access to a secure host was requested, then in step **2704** a further check is made to determine whether the user is authorized to connect to the secure host. Such a check can be made with reference to an internally stored list of authorized IP addresses, or can be made by communicating with gatekeeper **2603** (e.g., over an "administrative" VPN that is secure). It will be appreciated that different levels of security can also be provided for different categories of hosts. For example, some sites may be designated as having a certain security level, and the security level of the user requesting access must match that security level. The user's security level can also be determined by transmitting a request message back to the user's computer requiring that it prove that it has sufficient privileges.

If the user is not authorized to access the secure site, then a "host unknown" message is returned (step **2705**). If the user has sufficient security privileges, then in step **2706** a secure VPN is established between the user's computer and the secure target site. As described above, this is preferably done by allocating a hopping regime that will be carried out between the user's computer and the secure target site, and is preferably performed transparently to the user (i.e., the user need not be involved in creating the secure link). As described in various embodiments of this application, any of various fields can be "hopped" (e.g., IP source/destination addresses; a field in the header; etc.) in order to communicate securely.

Some or all of the security functions can be embedded in gatekeeper **2603**, such that it handles all requests to connect to secure sites. In this embodiment, DNS proxy **2610** communicates with gatekeeper **2603** to determine (preferably over a secure administrative VPN) whether the user has access to a particular web site. Various scenarios for implementing these features are described by way of example below:

Scenario #1: Client has permission to access target computer, and gatekeeper has a rule to make a VPN for the client. In this scenario, the client's DNS request would be received by the DNS proxy server **2610**, which would forward the request to gatekeeper **2603**. The gatekeeper would establish a VPN between the client and the requested target. The gatekeeper would provide the address of the destination to the DNS proxy, which would then return the resolved name as a result. The resolved address can be transmitted back to the client in a secure administrative VPN.

Scenario #2: Client does not have permission to access target computer. In this scenario, the client's DNS request would be received by the DNS proxy server **2610**, which would forward the request to gatekeeper **2603**. The gatekeeper would reject the request, informing DNS proxy server **2610** that it was unable to find the target computer. The DNS proxy **2610** would then return a "host unknown" error message to the client.

Scenario #3: Client has permission to connect using a normal non-VPN link, and the gatekeeper does not have a rule to set up a VPN for the client to the target site. In this scenario, the client's DNS request is received by DNS proxy server **2610**, which would check its rules and determine that no VPN is needed. Gatekeeper **2603** would then inform the DNS proxy server to forward the request to conventional DNS server **2609**, which would resolve the request and return the result to the DNS proxy server and then back to the client.

Scenario #4: Client does not have permission to establish a normal/non-VPN link, and the gatekeeper does not have a rule to make a VPN for the client to the target site. In this scenario, the DNS proxy server would receive the client's DNS request and forward it to gatekeeper **2603**. Gatekeeper **2603** would determine that no special VPN was needed, but that the client is not authorized to communicate with non-VPN members. The gatekeeper would reject the request, causing DNS proxy server **2610** to return an error message to the client.

C. Large Link to Small Link Bandwidth Management

One feature of the basic architecture is the ability to prevent so-called "denial of service" attacks that can occur if a computer hacker floods a known Internet node with packets, thus preventing the node from communicating with other nodes. Because IP addresses or other fields are "hopped" and packets arriving with invalid addresses are quickly discarded, Internet nodes are protected against flooding targeted at a single IP address.

In a system in which a computer is coupled through a link having a limited bandwidth (e.g., an edge router) to a node that can support a much higher-bandwidth link (e.g., an Internet Service Provider), a potential weakness could be exploited by a determined hacker. Referring to FIG. **28**, suppose that a first host computer **2801** is communicating with a second host computer **2804** using the IP address hopping principles described above. The first host computer is coupled through an edge router **2802** to an Internet Service Provider (ISP) **2803** through a low bandwidth link (LOW BW), and is in turn coupled to second host computer **2804** through parts of the Internet through a high bandwidth link (HIGH BW). In this architecture, the ISP is able to support a high bandwidth to the internet, but a much lower bandwidth to the edge router **2802**.

Suppose that a computer hacker is able to transmit a large quantity of dummy packets addressed to first host computer **2801** across high bandwidth link HIGH BW. Normally, host computer **2801** would be able to quickly reject the packets since they would not fall within the acceptance window

permitted by the IP address hopping scheme. However, because the packets must travel across low bandwidth link LOW BW, the packets overwhelm the lower bandwidth link before they are received by host computer **2801**. Consequently, the link to host computer **2801** is effectively flooded before the packets can be discarded.

According to one inventive improvement, a "link guard" function **2805** is inserted into the high-bandwidth node (e.g., ISP 2803) that quickly discards packets destined for a low-bandwidth target node if they are not valid packets. Each packet destined for a low-bandwidth node is cryptographically authenticated to determine whether it belongs to a VPN. If it is not a valid VPN packet, the packet is discarded at the high-bandwidth node. If the packet is authenticated as belonging to a VPN, the packet is passed with high preference. If the packet is a valid non-VPN packet, it is passed with a lower quality of service (e.g., lower priority).

In one embodiment, the ISP distinguishes between VPN and non-VPN packets using the protocol of the packet. In the case of IPSEC [rfc **2401**], the packets have IP protocols **420** and **421**. In the case of the TARP VPN, the packets will have an IP protocol that is not yet defined. The ISP's link guard, **2805**, maintains a table of valid VPNs which it uses to validate whether VPN packets are cryptographically valid. According to one embodiment, packets that do not fall within any hop windows used by nodes on the low-bandwidth link are rejected, or are sent with a lower quality of service. One approach for doing this is to provide a copy of the IP hopping tables used by the low-bandwidth nodes to the high-bandwidth node, such that both the high-bandwidth and low-bandwidth nodes track hopped packets (e.g., the high-bandwidth node moves its hopping window as valid packets are received). In such a scenario, the high-bandwidth node discards packets that do not fall within the hopping window before they are transmitted over the low-bandwidth link. Thus, for example, ISP **2903** maintains a copy **2910** of the receive table used by host computer **2901**. Incoming packets that do not fall within this receive table are discarded. According to a different embodiment, link guard **2805** validates each VPN packet using a keyed hashed message authentication code (HMAC) [rfc **2104**].

According to another embodiment, separate VPNs (using, for example, hopblocks) can be established for communicating between the low-bandwidth node and the high-bandwidth node (i.e., packets arriving at the high-bandwidth node are converted into different packets before being transmitted to the low-bandwidth node).

As shown in FIG. **29**, for example, suppose that a first host computer **2900** is communicating with a second host computer **2902** over the Internet, and the path includes a high bandwidth link HIGH BW to an ISP **2901** and a low bandwidth link LOW BW through an edge router **2904**. In accordance with the basic architecture described above, first host computer **2900** and second host computer **2902** would exchange hopblocks (or a hopblock algorithm) and would be able to create matching transmit and receive tables **2905**, **2906**, **2912** and **2913**. Then in accordance with the basic architecture, the two computers would transmit packets having seemingly random IP source and destination addresses, and each would move a corresponding hopping window in its receive table as valid packets were received.

Suppose that a nefarious computer hacker **2903** was able to deduce that packets having a certain range of IP addresses (e.g., addresses 100 to 200 for the sake of simplicity) are being transmitted to ISP **2901**, and that these packets are being forwarded over a low-bandwidth link. Hacker computer **2903** could thus "flood" packets having addresses falling into the range 100 to 200, expecting that they would be forwarded along low bandwidth link LOW BW, thus causing the low bandwidth link to become overwhelmed. The fast packet reject mechanism in first host computer **3000** would be of little use in rejecting these packets, since the low bandwidth link was effectively jammed before the packets could be rejected. In accordance with one aspect of the improvement, however, VPN link guard **2911** would prevent the attack from impacting the performance of VPN traffic because the packets would either be rejected as invalid VPN packets or given a lower quality of service than VPN traffic over the lower bandwidth link. A denial-of-service flood attack could, however, still disrupt non-VPN traffic.

According to one embodiment of the improvement, ISP **2901** maintains a separate VPN with first host computer **2900**, and thus translates packets arriving at the ISP into packets having a different IP header before they are transmitted to host computer **2900**. The cryptographic keys used to authenticate VPN packets at the link guard **2911** and the cryptographic keys used to encrypt and decrypt the VPN packets at host **2902** and host **2901** can be different, so that link guard **2911** does not have access to the private host data; it only has the capability to authenticate those packets.

According to yet a third embodiment, the low-bandwidth node can transmit a special message to the high-bandwidth node instructing it to shut down all transmissions on a particular IP address, such that only hopped packets will pass through to the low-bandwidth node. This embodiment would prevent a hacker from flooding packets using a single IP address. According to yet a fourth embodiment, the high-bandwidth node can be configured to discard packets transmitted to the low-bandwidth node if the transmission rate exceeds a certain predetermined threshold for any given IP address; this would allow hopped packets to go through. In this respect, link guard **2911** can be used to detect that the rate of packets on a given IP address are exceeding a threshold rate; further packets addressed to that same IP address would be dropped or transmitted at a lower priority (e.g., delayed).

D. Traffic Limiter

In a system in which multiple nodes are communicating using "hopping" technology, a treasonous insider could internally flood the system with packets. In order to prevent this possibility, one inventive improvement involves setting up "contracts" between nodes in the system, such that a receiver can impose a bandwidth limitation on each packet sender. One technique for doing this is to delay acceptance of a checkpoint synchronization request from a sender until a certain time period (e.g., one minute) has elapsed. Each receiver can effectively control the rate at which its hopping window moves by delaying "SYNC ACK" responses to "SYNC_REQ" messages.

A simple modification to the checkpoint synchronizer will serve to protect a receiver from accidental or deliberate overload from an internally treasonous client. This modification is based on the observation that a receiver will not update its tables until a SYNC_REQ is received on hopped address CKPT N. It is a simple matter of deferring the generation of a new CKPT_N until an appropriate interval after previous checkpoints.

Suppose a receiver wished to restrict reception from a transmitter to 100 packets a second, and that checkpoint synchronization messages were triggered every 50 packets. A compliant transmitter would not issue new SYNC_REQ

messages more often than every 0.5 seconds. The receiver could delay a non-compliant transmitter from synchronizing by delaying the issuance of CKPT_N for 0.5 second after the last SYNC_REQ was accepted.

In general, if M receivers need to restrict N transmitters issuing new SYNC_REQ messages after every W messages to sending R messages a second in aggregate, each receiver could defer issuing a new CKPT_N until MxNxW/R seconds have elapsed since the last SYNC_REQ has been received and accepted. If the transmitter exceeds this rate between a pair of checkpoints, it will issue the new checkpoint before the receiver is ready to receive it, and the SYNC_REQ will be discarded by the receiver. After this, the transmitter will re-issue the SYNC_REQ every T1 seconds until it receives a SYNC_ACK. The receiver will eventually update CKPT_N and the SYNC_REQ will be acknowledged. If the transmission rate greatly exceeds the allowed rate, the transmitter will stop until it is compliant. If the transmitter exceeds the allowed rate by a little, it will eventually stop after several rounds of delayed synchronization until it is in compliance. Hacking the transmitter's code to not shut off only permits the transmitter to lose the acceptance window. In this case it can recover the window and proceed only after it is compliant again.

Two practical issues should be considered when implementing the above scheme:

1. The receiver rate should be slightly higher than the permitted rate in order to allow for statistical fluctuations in traffic arrival times and non-uniform load balancing.

2. Since a transmitter will rightfully continue to transmit for a period after a SYNC_REQ is transmitted, the algorithm above can artificially reduce the transmitter's bandwidth. If events prevent a compliant transmitter from synchronizing for a period (e.g. the network dropping a SYNC_REQ or a SYNC_ACK) a SYNC_REQ will be accepted later than expected. After this, the transmitter will transmit fewer than expected messages before encountering the next checkpoint. The new checkpoint will not have been activated and the transmitter will have to retransmit the SYNC_REQ. This will appear to the receiver as if the transmitter is not compliant. Therefore, the next checkpoint will be accepted late from the transmitter's perspective. This has the effect of reducing the transmitter's allowed packet rate until the transmitter transmits at a packet rate below the agreed upon rate for a period of time.

To guard against this, the receiver should keep track of the times that the last C SYNC_REQs were received and accepted and use the minimum of MxNxW/R seconds after the last SYNC_REQ has been received and accepted, 2xMxNxW/R seconds after next to the last SYNC_REQ has been received and accepted, CxMxNxW/R seconds after $(C-1)^{th}$ to the last SYNC_REQ has been received, as the time to activate CKPT_N. This prevents the receiver from inappropriately limiting the transmitter's packet rate if at least one out of the last C SYNC_REQs was processed on the first attempt.

FIG. **30** shows a system employing the above-described principles. In FIG. **30**, two computers **3000** and **3001** are assumed to be communicating over a network N in accordance with the "hopping" principles described above (e.g., hopped IP addresses, discriminator values, etc.). For the sake of simplicity, computer **3000** will be referred to as the receiving computer and computer **3001** will be referred to as the transmitting computer, although full duplex operation is of course contemplated. Moreover, although only a single transmitter is shown, multiple transmitters can transmit to receiver **3000**.

As described above, receiving computer **3000** maintains a receive table **3002** including a window W that defines valid IP address pairs that will be accepted when appearing in incoming data packets. Transmitting computer **3001** maintains a transmit table **3003** from which the next IP address pairs will be selected when transmitting a packet to receiving computer **3000**. (For the sake of illustration, window W is also illustrated with reference to transmit table **3003**). As transmitting computer moves through its table, it will eventually generate a SYNC_REQ message as illustrated in function **3010**. This is a request to receiver **3000** to synchronize the receive table **3002**, from which transmitter **3001** expects a response in the form of a CKPT_N (included as part of a SYNC_ACK message). If transmitting computer **3001** transmits more messages than its allotment, it will prematurely generate the SYNC_REQ message. (If it has been altered to remove the SYNC_REQ message generation altogether, it will fall out of synchronization since receiver **3000** will quickly reject packets that fall outside of window W, and the extra packets generated by transmitter **3001** will be discarded).

In accordance with the improvements described above, receiving computer **3000** performs certain steps when a SYNC_REQ message is received, as illustrated in FIG. **30**. In step **3004**, receiving computer **3000** receives the SYNC_REQ message. In step **3005**, a check is made to determine whether the request is a duplicate. If so, it is discarded in step **3006**. In step **3007**, a check is made to determine whether the SYNC_REQ received from transmitter **3001** was received at a rate that exceeds the allowable rate R (i.e., the period between the time of the last SYNC_REQ message). The value R can be a constant, or it can be made to fluctuate as desired. If the rate exceeds R, then in step **3008** the next activation of the next CKPT_N hopping table entry is delayed by W/R seconds after the last SYNC_REQ has been accepted.

Otherwise, if the rate has not been exceeded, then in step **3109** the next CKPT_N value is calculated and inserted into the receiver's hopping table prior to the next SYNC_REQ from the transmitter **3101**. Transmitter **3101** then processes the SYNC_REQ in the normal manner.

E. Signaling Synchronizer

In a system in which a large number of users communicate with a central node using secure hopping technology, a large amount of memory must be set aside for hopping tables and their supporting data structures. For example, if one million subscribers to a web site occasionally communicate with the web site, the site must maintain one million hopping tables, thus using up valuable computer resources, even though only a small percentage of the users may actually be using the system at any one time. A desirable solution would be a system that permits a certain maximum number of simultaneous links to be maintained, but which would "recognize" millions of registered users at any one time. In other words, out of a population of a million registered users, a few thousand at a time could simultaneously communicate with a central server, without requiring that the server maintain one million hopping tables of appreciable size.

One solution is to partition the central node into two nodes: a signaling server that performs session initiation for user log-on and log-off (and requires only minimally sized tables), and a transport server that contains larger hopping tables for the users. The signaling server listens for the millions of known users and performs a fast-packet reject of other (bogus) packets. When a packet is received from a

Petitioner Apple Inc. - Exhibit 1002, p. 565

known user, the signaling server activates a virtual private link (VPL) between the user and the transport server, where hopping tables are allocated and maintained. When the user logs onto the signaling server, the user's computer is provided with hop tables for communicating with the transport server, thus activating the VPL. The VPLs can be torn down when they become inactive for a time period, or they can be torn down upon user log-out. Communication with the signaling server to allow user log-on and log-off can be accomplished using a specialized version of the checkpoint scheme described above.

FIG. **31** shows a system employing certain of the above-described principles. In FIG. **31**, a signaling server **3101** and a transport server **3102** communicate over a link. Signaling server **3101** contains a large number of small tables **3106** and **3107** that contain enough information to authenticate a communication request with one or more clients **3103** and **3104**. As described in more detail below, these small tables may advantageously be constructed as a special case of the synchronizing checkpoint tables described previously. Transport server **3102**, which is preferably a separate computer in communication with signaling server **3101**, contains a smaller number of larger hopping tables **3108**, **3109**, and **3110** that can be allocated to create a VPN with one of the client computers.

According to one embodiment, a client that has previously registered with the system (e.g., via a system administration function, a user registration procedure, or some other method) transmits a request for information from a computer (e.g., a web site). In one variation, the request is made using a "hopped" packet, such that signaling server **3101** will quickly reject invalid packets from unauthorized computers such as hacker computer **3105**. An "administrative" VPN can be established between all of the clients and the signaling server in order to ensure that a hacker cannot flood signaling server **3101** with bogus packets. Details of this scheme are provided below.

Signaling server **3101** receives the request **3111** and uses it to determine that client **3103** is a validly registered user. Next, signaling server **3101** issues a request to transport server **3102** to allocate a hopping table (or hopping algorithm or other regime) for the purpose of creating a VPN with client **3103**. The allocated hopping parameters are returned to signaling server **3101** (path **3113**), which then supplies the hopping parameters to client **3103** via path **3114**, preferably in encrypted form.

Thereafter, client **3103** communicates with transport server **3102** using the normal hopping techniques described above. It will be appreciated that although signaling server **3101** and transport server **3102** are illustrated as being two separate computers, they could of course be combined into a single computer and their functions performed on the single computer. Alternatively, it is possible to partition the functions shown in FIG. **31** differently from as shown without departing from the inventive principles.

One advantage of the above-described architecture is that signaling server **3101** need only maintain a small amount of information on a large number of potential users, yet it retains the capability of quickly rejecting packets from unauthorized users such as hacker computer **3105**. Larger data tables needed to perform the hopping and synchronization functions are instead maintained in a transport server **3102**, and a smaller number of these tables are needed since they are only allocated for "active" links. After a VPN has become inactive for a certain time period (e.g., one hour), the VPN can be automatically torn down by transport server **3102** or signaling server **3101**.

A more detailed description will now be provided regarding how a special case of the checkpoint synchronization feature can be used to implement the signaling scheme described above.

The signaling synchronizer may be required to support many (millions) of standing, low bandwidth connections. It therefore should minimize per-VPL memory usage while providing the security offered by hopping technology. In order to reduce memory usage in the signaling server, the data hopping tables can be completely eliminated and data can be carried as part of the SYNC_REQ message. The table used by the server side (receiver) and client side (transmitter) is shown schematically as element **3106** in FIG. **31**.

The meaning and behaviors of CKPT_N, CKPT_O and CKPT_R remain the same from the previous description, except that CKPT_N can receive a combined data and SYNC_REQ message or a SYNC_REQ message without the data.

The protocol is a straightforward extension of the earlier synchronizer. Assume that a client transmitter is on and the tables are synchronized. The initial tables can be generated "out of band." For example, a client can log into a web server to establish an account over the Internet. The client will receive keys etc encrypted over the Internet. Meanwhile, the server will set up the signaling VPN on the signaling server.

Assuming that a client application wishes to send a packet to the server on the client's standing signaling VPL:

1. The client sends the message marked as a data message on the inner header using the transmitter's CKPT_N address. It turns the transmitter off and starts a timer T1 noting CKP_O. Messages can be one of three types: DATA, SYNC_REQ and SYNC_ACK. In the normal algorithm, some potential problems can be prevented by identifying each message type as part of the encrypted inner header field. In this algorithm, it is important to distinguish a data packet and a SYNC_REQ in the signaling synchronizer since the data and the SYNC_REQ come in on the same address.

2. When the server receives a data message on its CKPT_N, it verifies the message and passes it up the stack. The message can be verified by checking message type and and other information (i.e., user credentials) contained in the inner header It replaces its CKPT_O with CKPT_N and generates the next CKPT_N. It updates its transmitter side CKPT_R to correspond to the client's receiver side CKPT_R and transmits a SYNC_ACK containing CKPT_O in its payload.

3. When the client side receiver receives a SYNC_ACK on its CKPT_R with a payload matching its transmitter side CKPT_O and the transmitter is off, the transmitter is turned on and the receiver side CKPT_R is updated. If the SYNC_ACK's payload does not match the transmitter side CKPT_O or the transmitter is on, the SYNC_ACK is simply discarded.

4. T1 expires: If the transmitter is off and the client's transmitter side CKPT_O matches the CKPT_O associated with the timer, it starts timer T1 noting CKPT_O again, and a SYNC_REQ is sent using the transmitter's CKPT_O address. Otherwise, no action is taken.

5. When the server receives a SYNC_REQ on its CKPT_N, it replaces its CKPT_O with CKPT_N and generates the next CKPT _N. It updates its transmitter side CKPT_R to correspond to the client's receiver side CKPT_R and transmits a SYNC_ACK containing CKPT_O in its payload.

6. When the server receives a SYNC_REQ on its CKPT_O, it updates its transmitter side CKPT_R to correspond to the client's receiver side CKPT_R and transmits a SYNC_ACK containing CKPT_O in its payload.

FIG. **32** shows message flows to highlight the protocol. Reading from top to bottom, the client sends data to the server using its transmitter side CKPT_N. The client side transmitter is turned off and a retry timer is turned off. The transmitter will not transmit messages as long as the transmitter is turned off. The client side transmitter then loads CKPT_N into CKPT_O and updates CKPT_N. This message is successfully received and a passed up the stack. It also synchronizes the receiver i.e., the server loads CKPT_N into CKPT_O and generates a new CKPT_N, it generates a new CKPT_R in the server side transmitter and transmits a SYNC_ACK containing the server side receiver's CKPT_O the server. The SYNC_ACK is successfully received at the client. The client side receiver's CKPT_R is updated, the transmitter is turned on and the retry timer is killed. The client side transmitter is ready to transmit a new data message.

Next, the client sends data to the server using its transmitter side CKPT_N. The client side transmitter is turned off and a retry timer is turned off. The transmitter will not transmit messages as long as the transmitter is turned off. The client side transmitter then loads CKPT_N into CKPT_O and updates CKPT_N. This message is lost. The client side timer expires and as a result a SYNC_REQ is transmitted on the client side transmitter's CKPT_O (this will keep happening until the SYNC_ACK has been received at the client). The SYNC_REQ is successfully received at the server. It synchronizes the receiver i.e., the server loads CKPT_N into CKPT_O and generates a new CKPT_N, it generates an new CKPT_R in the server side transmitter and transmits a SYNC_ACK containing the server side receiver's CKPT_O the server. The SYNC_ACK is successfully received at the client. The client side receiver's CKPT_R is updated, the transmitter is turned off and the retry timer is killed. The client side transmitter is ready to transmit a new data message.

There are numerous other scenarios that follow this flow. For example, the SYNC_ACK could be lost. The transmitter would continue to re-send the SYNC_REQ until the receiver synchronizes and responds.

The above-described procedures allow a client to be authenticated at signaling server **3201** while maintaining the ability of signaling server **3201** to quickly reject invalid packets, such as might be generated by hacker computer **3205**. In various embodiments, the signaling synchronizer is really a derivative of the synchronizer. It provides the same protection as the hopping protocol, and it does so for a large number of low bandwidth connections.

F. One-Click Secure On-Line Communications and Secure Domain Name Service

The present invention provides a technique for establishing a secure communication link between a first computer and a second computer over a computer network. Preferably, a user enables a secure communication link using a single click of a mouse, or a corresponding minimal input from another input device, such as a keystroke entered on a keyboard or a click entered through a trackball. Alternatively, the secure link is automatically established as a default setting at boot-up of the computer (i.e., no click). FIG. **33** shows a system block diagram **3300** of a computer network in which the one-click secure communication method of the present invention is suitable. In FIG. **33**, a computer terminal or client computer **3301**, such as a personal computer (PC), is connected to a computer network **3302**, such as the Internet, through an ISP **3303**. Alternatively, computer **3301** can be connected to computer network **3302** through an edge router. Computer **3301** includes an input device, such as a keyboard and/or mouse, and a display device, such as a monitor. Computer **3301** can communicate conventionally with another computer **3304** connected to computer network **3302** over a communication link **3305** using a browser **3306** that is installed and operates on computer **3301** in a well-known manner.

Computer **3304** can be, for example, a server computer that is used for conducting e-commerce. In the situation when computer network **3302** is the Internet, computer **3304** typically will have a standard top-level domain name such as .com, .net, .org, .edu, .mil or .gov.

FIG. **34** shows a flow diagram **3400** for installing and establishing a "one-click" secure communication link over a computer network according to the present invention. At step **3401**, computer **3301** is connected to server computer **3304** over a non-VPN communication link **3305**. Web browser **3306** displays a web page associated with server **3304** in a well-known manner. According to one variation of the invention, the display of computer **3301** contains a hyperlink, or an icon representing a hyperlink, for selecting a virtual private network (VPN) communication link ("go secure" hyperlink) through computer network **3302** between terminal **3301** and server **3304**. Preferably, the "go secure" hyperlink is displayed as part of the web page downloaded from server computer **3304**, thereby indicating that the entity providing server **3304** also provides VPN capability.

By displaying the "go secure" hyperlink, a user at computer **3301** is informed that the current communication link between computer **3301** and server computer **3304** is a non-secure, non-VPN communication link. At step **3402**, it is determined whether a user of computer **3301** has selected the "go secure" hyperlink. If not, processing resumes using a non-secure (conventional) communication method (not shown). If, at step **3402**, it is determined that the user has selected the "go secure" hyperlink, flow continues to step **3403** where an object associated with the hyperlink determines whether a VPN communication software module has already been installed on computer **3301**. Alternatively, a user can enter a command into computer **3301** to "go secure."

If, at step **3403**, the object determines that the software module has been installed, flow continues to step **3407**. If, at step **3403**, the object determines that the software module has not been installed, flow continues to step **3404** where a non-VPN communication link **3307** is launched between computer **3301** and a website **3308** over computer network **3302** in a well-known manner. Website **3308** is accessible by all computer terminals connected to computer network **3302** through a non-VPN communication link. Once connected to website **3308**, a software module for establishing a secure communication link over computer network **3302** can be downloaded and installed. Flow continues to step **3405** where, after computer **3301** connects to website **3308**, the software module for establishing a communication link is downloaded and installed in a well-known manner on computer terminal **3301** as software module **3309**. At step **3405**, a user can optionally select parameters for the software module, such as enabling a secure communication link mode of communication for all communication links over com-

puter network **3302**. At step **3406**, the communication link between computer **3301** and website **3308** is then terminated in a well-known manner.

By clicking on the "go secure" hyperlink, a user at computer **3301** has enabled a secure communication mode of communication between computer **3301** and server computer **3304**. According to one variation of the invention, the user is not required to do anything more than merely click the "go secure" hyperlink. The user does not need to enter any user identification information, passwords or encryption keys for establishing a secure communication link. All procedures required for establishing a secure communication link between computer **3301** and server computer **3304** are performed transparently to a user at computer **3301**.

At step **3407**, a secure VPN communications mode of operation has been enabled and software module **3309** begins to establish a VPN communication link. In one embodiment, software module **3309** automatically replaces the top-level domain name for server **3304** within browser **3406** with a secure top-level domain name for server computer **3304**. For example, if the top-level domain name for server **3304** is .com, software module **3309** replaces the .com top-level domain name with a .scom top-level domain name, where the "s" stands for secure. Alternatively, software module **3409** can replace the top-level domain name of server **3304** with any other non-standard top-level domain name.

Because the secure top-level domain name is a non-standard domain name, a query to a standard domain name service (DNS) will return a message indicating that the universal resource locator (URL) is unknown. According to the invention, software module **3409** contains the URL for querying a secure domain name service (SDNS) for obtaining the URL for a secure top-level domain name. In this regard, software module **3309** accesses a secure portal **3310** that interfaces a secure network **3311** to computer network **3302**. Secure network **3311** includes an internal router **3312**, a secure domain name service (SDNS) **3313**, a VPN gatekeeper **3314** and a secure proxy **3315**. The secure network can include other network services, such as e-mail **3316**, a plurality of chatrooms (of which only one chatroom **3317** is shown), and a standard domain name service (STD DNS) **3318**. Of course, secure network **3311** can include other resources and services that are not shown in FIG. **33**.

When software module **3309** replaces the standard top-level domain name for server **3304** with the secure top-level domain name, software module **3309** sends a query to SDNS **3313** at step **3408** through secure portal **3310** preferably using an administrative VPN communication link **3319**. In this configuration, secure portal **3310** can only be accessed using a VPN communication link. Preferably, such a VPN communication link can be based on a technique of inserting a source and destination IP address pair into each data packet that is selected according to a pseudo-random sequence; an IP address hopping regime that pseudorandomly changes IP addresses in packets transmitted between a client computer and a secure target computer; periodically changing at least one field in a series of data packets according to a known sequence; an Internet Protocol (IP) address in a header of each data packet that is compared to a table of valid IP addresses maintained in a table in the second computer; and/or a comparison of the IP address in the header of each data packet to a moving window of valid IP addresses, and rejecting data packets having IP addresses that do not fall within the moving window. Other types of VPNs can alternatively be used. Secure portal **3310** authenticates the query from software module **3309** based on the particular information hopping technique used for VPN communication link **3319**.

SDNS **3313** contains a cross-reference database of secure domain names and corresponding secure network addresses. That is, for each secure domain name, SDNS **3313** stores a computer network address corresponding to the secure domain name. An entity can register a secure domain name in SDNS **3313** so that a user who desires a secure communication link to the website of the entity can automatically obtain the secure computer network address for the secure website. Moreover, an entity can register several secure domain names, with each respective secure domain name representing a different priority level of access in a hierarchy of access levels to a secure website. For example, a securities trading website can provide users secure access so that a denial of service attack on the website will be ineffectual with respect to users subscribing to the secure website service. Different levels of subscription can be arranged based on, for example, an escalating fee, so that a user can select a desired level of guarantee for connecting to the secure securities trading website. When a user queries SDNS **3313** for the secure computer network address for the securities trading website, SDNS **3313** determines the particular secure computer network address based on the user's identity and the user's subscription level.

At step **3409**, SDNS **3313** accesses VPN gatekeeper **3314** for establishing a VPN communication link between software module **3309** and secure server **3320**. Server **3320** can only be accessed through a VPN communication link. VPN gatekeeper **3314** provisions computer **3301** and secure web server computer **3320**, or a secure edge router for server computer **3320**, thereby creating the VPN. Secure server computer **3320** can be a separate server computer from server computer **3304**, or can be the same server computer having both non-VPN and VPN communication link capability, such as shown by server computer **3322**. Returning to FIG. **34**, in step **3410**, SDNS **3313** returns a secure URL to software module **3309** for the .scom server address for a secure server **3320** corresponding to server **3304**.

Alternatively, SDNS **3313** can be accessed through secure portal **3310** "in the clear", that is, without using an administrative VPN communication link. In this situation, secure portal **3310** preferably authenticates the query using any well-known technique, such as a cryptographic technique, before allowing the query to proceed to SDNS **3319**. Because the initial communication link in this situation is not a VPN communication link, the reply to the query can be "in the clear." The querying computer can use the clear reply for establishing a VPN link to the desired domain name. Alternatively, the query to SDNS **3313** can be in the clear, and SDNS **3313** and gatekeeper **3314** can operate to establish a VPN communication link to the querying computer for sending the reply.

At step **3411**, software module **3309** accesses secure server **3320** through VPN communication link **3321** based on the VPN resources allocated by VPN gatekeeper **3314**. At step **3412**, web browser **3306** displays a secure icon indicating that the current communication link to server **3320** is a secure VPN communication link. Further communication between computers **3301** and **3320** occurs via the VPN, e.g., using a "hopping" regime as discussed above. When VPN link **3321** is terminated at step **3413**, flow continues to step **3414** where software module **3309** automatically replaces the secure top-level domain name with the corresponding non-secure top-level domain name for server **3304**. Browser **3306** accesses a standard DNS **3325** for obtaining the

Petitioner Apple Inc. - Exhibit 1002, p. 568

non-secure URL for server **3304**. Browser **3306** then connects to server **3304** in a well-known manner. At step **3415**, browser **3306** displays the "go secure" hyperlink or icon for selecting a VPN communication link between terminal **3301** and server **3304**. By again displaying the "go secure" hyperlink, a user is informed that the current communication link is a non-secure, non-VPN communication link.

When software module **3309** is being installed or when the user is off-line, the user can optionally specify that all communication links established over computer network **3302** are secure communication links. Thus, anytime that a communication link is established, the link is a VPN link. Consequently, software module **3309** transparently accesses SDNS **3313** for obtaining the URL for a selected secure website. In other words, in one embodiment, the user need not "click" on the secure option each time secure communication is to be effected.

Additionally, a user at computer **3301** can optionally select a secure communication link through proxy computer **3315**. Accordingly, computer **3301** can establish a VPN communication link **3323** with secure server computer **3320** through proxy computer **3315**. Alternatively, computer **3301** can establish a non-VPN communication link **3324** to a non-secure website, such as non-secure server computer **3304**.

FIG. **35** shows a flow diagram **3500** for registering a secure domain name according to the present invention. At step **3501**, a requester accesses website **3308** and logs into a secure domain name registry service that is available through website **3308**. At step **3502**, the requestor completes an online registration form for registering a secure domain name having a top-level domain name, such as .com, .net, .org, .edu, .mil or .gov. Of course, other secure top-level domain names can also be used. Preferably, the requestor must have previously registered a non-secure domain name corresponding to the equivalent secure domain name that is being requested. For example, a requester attempting to register secure domain name "website.scom" must have previously registered the corresponding non-secure domain name "website.com".

At step **3503**, the secure domain name registry service at website **3308** queries a non-secure domain name server database, such as standard DNS **3322**, using, for example, a whois query, for determining ownership information relating to the non-secure domain name corresponding to the requested secure domain name. At step **3504**, the secure domain name registry service at website **3308** receives a reply from standard DNS **3322** and at step **3505** determines whether there is conflicting ownership information for the corresponding non-secure domain name. If there is no conflicting ownership information, flow continues to step **3507**, otherwise flow continues to step **3506** where the requestor is informed of the conflicting ownership information. Flow returns to step **3502**.

When there is no conflicting ownership information at step **3505**, the secure domain name registry service (website **3308**) informs the requestor that there is no conflicting ownership information and prompts the requester to verify the information entered into the online form and select an approved form of payment. After confirmation of the entered information and appropriate payment information, flow continues to step **3508** where the newly registered secure domain name sent to SDNS **3313** over communication link **3326**.

If, at step **3505**, the requested secure domain name does not have a corresponding equivalent non-secure domain name, the present invention informs the requestor of the situation and prompts the requestor for acquiring the corresponding equivalent non-secure domain name for an increased fee. By accepting the offer, the present invention automatically registers the corresponding equivalent non-secure domain name with standard DNS **3325** in a well-known manner. Flow then continues to step **3508**.

G. Tunneling Secure Address Hopping Protocol Through Existing Protocol Using Web Proxy

The present invention also provides a technique for implementing the field hopping schemes described above in an application program on the client side of a firewall between two computer networks, and in the network stack on the server side of the firewall. The present invention uses a new secure connectionless protocol that provides good denial of service rejection capabilities by layering the new protocol on top of an existing IP protocol, such as the ICMP, UDP or TCP protocols. Thus, this aspect of the present invention does not require changes in the Internet infrastructure.

According to the invention, communications are protected by a client-side proxy application program that accepts unencrypted, unprotected communication packets from a local browser application. The client-side proxy application program tunnels the unencrypted, unprotected communication packets through a new protocol, thereby protecting the communications from a denial of service at the server side. Of course, the unencrypted, unprotected communication packets can be encrypted prior to tunneling.

The client-side proxy application program is not an operating system extension and does not involve any modifications to the operating system network stack and drivers. Consequently, the client is easier to install, remove and support in comparison to a VPN. Moreover, the client-side proxy application can be allowed through a corporate firewall using a much smaller "hole" in the firewall and is less of a security risk in comparison to allowing a protocol layer VPN through a corporate firewall.

The server-side implementation of the present invention authenticates valid field-hopped packets as valid or invalid very early in the server packet processing, similar to a standard virtual private network, for greatly minimizing the impact of a denial of service attempt in comparison to normal TCP/IP and HTTP communications, thereby protecting the server from invalid communications.

FIG. **36** shows a system block diagram of a computer network **3600** in which a virtual private connection according to the present invention can be configured to more easily traverse a firewall between two computer networks. FIG. **37** shows a flow diagram **3700** for establishing a virtual private connection that is encapsulated using an existing network protocol.

In FIG. **36** a local area network (LAN) **3601** is connected to another computer network **3602**, such as the Internet, through a firewall arrangement **3603**. Firewall arrangement operates in a well-known manner to interface LAN **3601** to computer network **3602** and to protect LAN **3601** from attacks initiated outside of LAN **3601**.

A client computer **3604** is connected to LAN **3601** in a well-known manner. Client computer **3604** includes an operating system **3605** and a web browser **3606**. Operating system **3605** provides kernel mode functions for operating client computer **3604**. Browser **3606** is an application program for accessing computer network resources connected to LAN **3601** and computer network **3602** in a well-known manner. According to the present invention, a proxy application **3607** is also stored on client computer **3604** and

Petitioner Apple Inc. - Exhibit 1002, p. 569

operates at an application layer in conjunction with browser **3606**. Proxy application **3607** operates at the application layer within client computer **3604** and when enabled, modifies unprotected, unencrypted message packets generated by browser **3606** by inserting data into the message packets that are used for forming a virtual private connection between client computer **3604** and a server computer connected to LAN **3601** or computer network **3602**. According to the invention, a virtual private connection does not provide the same level of security to the client computer as a virtual private network. A virtual private connection can be conveniently authenticated so that, for example, a denial of service attack can be rapidly rejected, thereby providing different levels of service that can be subscribed to by a user.

Proxy application **3607** is conveniently installed and uninstalled by a user because proxy application **3607** operates at the application layer within client computer **3604**. On installation, proxy application **3607** preferably configures browser **3606** to use proxy application for all web communications. That is, the payload portion of all message packets is modified with the data for forming a virtual private connection between client computer **3604** and a server computer. Preferably, the data for forming the virtual private connection contains field-hopping data, such as described above in connection with VPNs. Also, the modified message packets preferably conform to the UDP protocol. Alternatively, the modified message packets can conform to the TCP/IP protocol or the ICMP protocol. Alternatively, proxy application **3606** can be selected and enabled through, for example, an option provided by browser **3606**. Additionally, proxy application **3607** can be enabled so that only the payload portion of specially designated message packets is modified with the data for forming a virtual private connection between client computer **3604** and a designated host computer. Specially designated message packets can be, for example, selected predetermined domain names.

Referring to FIG. **37**, at step **3701**, unprotected and unencrypted message packets are generated by browser **3606**. At step **3702**, proxy application **3607** modifies the payload portion of all message packets by tunneling the data for forming a virtual private connection between client computer **3604** and a destination server computer into the payload portion. At step, **3703**, the modified message packets are sent from client computer **3604** to, for example, website (server computer) **3608** over computer network **3602**.

Website **3608** includes a VPN guard portion **3609**, a server proxy portion **3610** and a web server portion **3611**. VPN guard portion **3609** is embedded within the kernel layer of the operating system of website **3608** so that large bandwidth attacks on website **3608** are rapidly rejected. When client computer **3604** initiates an authenticated connection to website **3608**, VPN guard portion **3609** is keyed with the hopping sequence contained in the message packets from client computer **3604**, thereby performing a strong authentication of the client packet streams entering website **3608** at step **3704**. VPN guard portion **3609** can be configured for providing different levels of authentication and, hence, quality of service, depending upon a subscribed level of service. That is, VPN guard portion **3609** can be configured to let all message packets through until a denial of service attack is detected, in which case VPN guard portion **3609** would allow only client packet streams conforming to a keyed hopping sequence, such as that of the present invention.

Server proxy portion **3610** also operates at the kernel layer within website **3608** and catches incoming message packets from client computer **3604** at the VPN level. At step **3705**, server proxy portion **3610** authenticates the message packets at the kernel level within host computer **3604** using the destination IP address, UDP ports and discriminator fields. The authenticated message packets are then forwarded to the authenticated message packets to web server portion **3611** as normal TCP web transactions.

At step **3705**, web server portion **3611** responds to message packets received from client computer **3604** in accordance with the particular nature of the message packets by generating reply message packets. For example, when a client computer requests a webpage, web server portion **3611** generates message packets corresponding to the requested webpage. At step **3706**, the reply message packets pass through server proxy portion **3610**, which inserts data into the payload portion of the message packets that are used for forming the virtual private connection between host computer **3608** and client computer **3604** over computer network **3602**. Preferably, the data for forming the virtual private connection is contains field-hopping data, such as described above in connection with VPNs. Server proxy portion **3610** operates at the kernel layer within host computer **3608** to insert the virtual private connection data into the payload portion of the reply message packets. Preferably, the modified message packets sent by host computer **3608** to client computer **3604** conform to the UDP protocol. Alternatively, the modified message packets can conform to the TCP/IP protocol or the ICMP protocol.

At step **3707**, the modified packets are sent from host computer **3608** over computer network **3602** and pass through firewall **3603**. Once through firewall **3603**, the modified packets are directed to client computer **3604** over LAN **3601** and are received at step **3708** by proxy application **3607** at the application layer within client computer **3604**. Proxy application **3607** operates to rapidly evaluate the modified message packets for determining whether the received packets should be accepted or dropped. If the virtual private connection data inserted into the received information packets conforms to expected virtual private connection data, then the received packets are accepted. Otherwise, the received packets are dropped.

While the present invention has been described in connection with the illustrated embodiments, it will be appreciated and understood that modifications may be made without departing from the true spirit and scope of the invention.

What is claimed is:

1. A method for accessing a secure computer network address, comprising steps of:

receiving a secure domain name;

sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;

receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and

sending an access request message to the secure computer network address using a virtual private network communication link.

2. The method according to claim **1**, wherein the step of receiving the secure domain name includes steps of:

receiving a command to establish the virtual private network communication link with a secure computer network address corresponding to a predetermined non-secure domain name; and

automatically generating a secure domain name corresponding to the non-secure domain name.

3. The method according to claim 2, wherein the step of receiving a command to establish the virtual private network communication link includes a step of selecting a predetermined icon displayed on a computer display.

4. The method according to claim 1, wherein the response message contains provisioning information for the virtual private network.

5. The method according to claim 4, wherein the virtual private network is based on inserting one or more data values into each data packet sent to the secure computer network address, the one or more data values varying according to a pseudo-random sequence.

6. The method according to claim 4, wherein the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network.

7. The method according to claim 4, wherein the virtual private network is based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses in packets transmitted between a first computer and a second computer.

8. The method according to claim 4, wherein the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values.

9. The method according to claim 4, wherein the virtual private network is based on a comparison of a discriminator field in a header of each data packet to the secure computer network address to a table of valid discriminator fields.

10. The method according to claim 1, wherein the virtual private network includes the Internet.

11. The method according to claim 1, wherein the secure domain name has a top-level domain name that includes one of .scom, .snet, .sorg, .sedu, .smil or .sgov.

12. The method of claim 1, wherein the access request message contains a request for information stored at the secure computer network address.

13. The method of claim 1,

wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;

wherein sending the query message comprises sending the query message at the client computer;

wherein receiving the response message comprises receiving the response message at the client computer,

wherein sending the access request message comprises sending the access request message at the client computer.

14. The method of claim 1, performed by a software module.

15. The method of claim 1, performed by a client computer.

16. The method of claim 2, wherein receiving the command comprises receiving the command at a client computer from a user.

17. A computer-readable storage medium, comprising:

a storage area; and

computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:

receiving a secure domain name;

sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain name;

receiving from the domain name service a response message containing the secure computer network address corresponding to the secure domain name; and

sending an access request message to the secure computer network address using a virtual private network communication link.

18. The computer-readable medium according to claim 17, wherein the step of receiving the secure domain name includes steps of:

receiving a command to establish the virtual private network communication link with a secure computer network address corresponding to a predetermined non-secure domain name; and

automatically generating a secure domain name corresponding to the non-secure domain name.

19. The computer-readable medium according to claim 18, wherein the step of receiving a command to establish the virtual private network communication link includes a step of selecting a predetermined icon displayed on a computer display.

20. The computer-readable medium according to claim 17, wherein the response message contains provisioning information for the virtual private network.

21. The computer-readable medium according to claim 20, wherein the virtual private network is based on inserting one or more data values into each data packet sent to the secure computer network address, the one or more data values varying according to a pseudo-random sequence.

22. The computer-readable medium according to claim 20, wherein the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network.

23. The computer-readable medium according to claim 20, wherein the virtual private network is based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses in packets transmitted between a first computer and a second computer.

24. The computer-readable medium according to claim 20, wherein the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values.

25. The computer-readable medium according to claim 20, wherein the virtual private network is based on a comparison of a discriminator field in a header of each data packet to the secure computer network address to a table of valid discriminator fields.

26. The computer-readable medium according to claim 17, wherein the virtual private network includes the Internet.

27. The computer-readable medium according to claim 17, wherein the secure domain name has a top-level domain name that includes one of .scom, .snet, .sorg, .sedu, .smil or .sgov.

28. The computer readable medium of claim 17, wherein the access request message contains a request for information stored at the secure computer network address.

29. The computer-readable medium according to claim 17,

wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;

wherein sending the query message comprises sending the query message at the client computer;

wherein receiving the response message comprises receiving the response message at the client computer,

wherein sending the access request message comprises sending the access request message at the client computer.

30. The computer-readable medium according to claim 17, wherein the method is performed by a software module.

31. The computer-readable medium according to claim 17, wherein the method is performed by a client computer.

32. The computer-readable medium according to claim 18, wherein receiving the command comprises receiving the command at a client computer from a user.

33. A data processing apparatus, comprising:

a processor, and

memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:

receiving a secure domain name;

sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;

receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and

sending an access request message to the secure computer network address using a virtual private network communication link.

34. The apparatus of claim 33, wherein the step of receiving the secure domain name includes steps of:

receiving a command to establish the virtual private network communication link with a secure computer network address corresponding to a predetermined non-secure domain name; and

automatically generating a secure domain name corresponding to the non-secure domain name.

35. The apparatus of claim 33, wherein the response message contains provisioning information for the virtual private network.

36. The apparatus of claim 35, wherein the virtual private network is based on inserting one or more data values into each data packet sent to the secure computer network address, the one or more data values varying according to a pseudo-random sequence.

37. The apparatus of claim 35, wherein the virtual private network is based on inserting into at least one data packet at least one data value representing a predetermined level of service associated with the virtual private network.

38. The apparatus of claim 35, wherein the virtual private network is based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses in packets transmitted between a first computer and a second computer.

39. The apparatus of claim 35, wherein the virtual private network is based on comparing a value in each data packet transmitted to the secure computer network address to a moving window of valid values.

40. The apparatus of claim 35, wherein the virtual private network is based on a comparison of a discriminator field in a header of each data packet to the secure computer network address to a table of valid discriminator fields.

41. The apparatus of claim 33, wherein the secure domain name has a top-level domain name that includes one of scom, .snet, .sorg, .sedu, smil or .sgov.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 7,188,180 B2
APPLICATION NO. : 10/702486
DATED : March 6, 2007
INVENTOR(S) : Victor Larson et al.

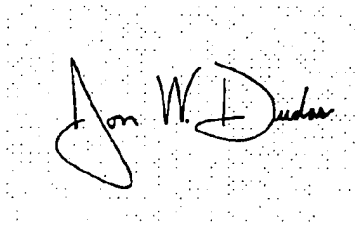
It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

IN PATENT TITLE PAGE:

Item (75), Inventors, delete "Durham" and insert therefor – Dunham --.

Signed and Sealed this

Seventh Day of August, 2007



JON W. DUDAS
Director of the United States Patent and Trademark Office

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTC/SB/08a (01-09)
Approved for use through 02/28/2009. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	2009-11-25
	First Named Inventor	LARSON, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	3755-121

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS								
Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

EFS Web 2.1.10

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	2009-11-25
	First Named Inventor	LARSON, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	3755-121

	1	Exhibit 2 "Aventail Connect v3.1/v2.6 Administrator's Guide", pgs. 1-120, 1996-1999.	☐
	2	Exhibit 3, "Windows NT Server, Virtual Private Network: An Overview", pgs. 1-28, 1998.	☐
	3	Exhibit 4, "Network Working Group Request For Comments 1035", pgs. 1-56, 1987.	☐
	4	Exhibit 5, "Kustur" Building and Managing Virtual Private Networks, pgs 1-396, 1998.	☐
	5	Exhibit 6, "Kaufman et al.," Implementing IPsec, pgs. 1-280, 1999.	☐
	6	Exhibit 7, "James Galvin" Public Key Distribution Secure DNS, pgs. 1-12, 1996.	☐
	7	Exhibit 8A, "Gauntlet Firewall for Windows NT Administrator's Guide, pgs 1-137, 1998-1999.	☐
	8	Exhibit 8B, "Gauntlet Firewall for Windows NT Administrator's Guide, pgs. 138-275, 1998-1999.	☐
	9	Exhibit 9, "Windows NT Technical Support: Hands On, Self Paced Training for Supporting Version 4.0", pgs. 1-106, 1998.	☐
	10	Exhibit 10, "Microsoft Windows NT Server, Whitepaper: Installing, Configuring, and Using PPTP with Mircosoft Clients and Servers, pgs. 1-30, 1997.	☐
	11	Exhibit 11, "Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources, pgs. 1-216, 2000.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	2009-11-25
	First Named Inventor	LARSON, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	3755-121

If you wish to add additional non-patent literature document citation information please click the Add button			
EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	2009-11-25
	First Named Inventor	LARSON, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	3755-121

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

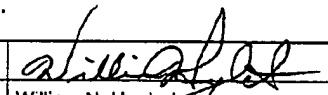
☐ See attached certification statement.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature		Date (YYYY-MM-DD)	2009-11-25
Name/Print	William N. Hughet	Registration Number	44481

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

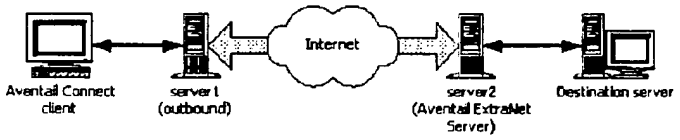
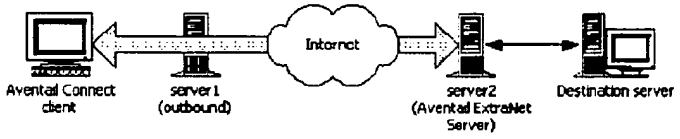
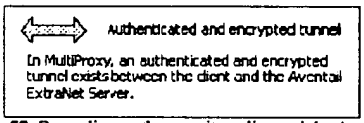
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Appendix A

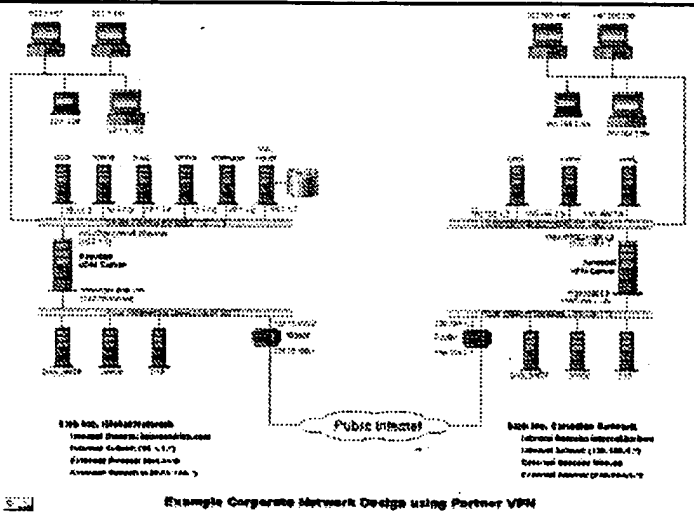
Citations to Exemplary Description in the Aventail Connect v3.1/v2.6 Administrator's Guide Reference*

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
1. A method for accessing a secure computer network address, comprising steps of:	Page 6: Escalating security threats are forcing companies to seek ways to safeguard their corporate networks and the information they exchange. The first response to these concerns has been the development of security firewalls—software barriers that control the flow of information. But firewalls are not designed to handle complex security issues, such as monitoring network usage, providing private communication over public networks, and enabling remote users to gain secure access to internal network resources. Page 12: b. When the connection is completed, Aventail Connect begins the SOCKS negotiation. • It sends the list of authentication methods enabled in the configuration file • Once the server selects an authentication method, Aventail Connect executes the specified authentication processing. • It then sends the proxy request to the extranet (SOCKS) server. This includes either the IP address provided by the application or the DNS entry (hostname) provided in step 1. Page 46: SOCKS v5 servers often require user authentication before allowing access. Aventail Connect authentication modules display dialog boxes that prompt users to enter username and password information as well as other authentication credentials. The current Aventail Connect authentication modules are SOCKS v4 Identification, Username / Password, Challenge Handshake Authentication Protocol (CHAP), Challenge Response Authentication Method (CRAM), Secure Sockets Layer (SSL), and HTTP Basic (username/password). Page 62: Once servers and destinations are defined, you can direct SOCKS traffic through successive extranet (SOCKS) servers. Page 66: To gain access to your extranet, users may need to traverse multiple firewalls. In the simplest case, this involves an employee at a partner company gaining access to the Internet via an outbound proxy server at the partner company, and having an authenticated, encrypted, and controlled connection to your internal network via an Aventail ExtraNet Server. This capability is provided in Aventail Connect 3.1 by the Aventail MultiProxy feature. Aventail Connect can open connections through SOCKS servers, through HTTP proxies, or through proxy chaining. Page 72:

* - The cited passages are an indication of where in the Aventail reference, at the very least, the claims find exemplary description. Requestor reserves the right to identify and demonstrate additional description if necessary or desirable.

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	PROXY CHAINING: Server1 appears as a user to server2.  **MULTIPROXY:** The user authenticates with server2 directly.   Page 77: Depending on the security policy and the Aventail ExtraNet Server configuration, Aventail Connect will automatically proxy their allowed application traffic into the private network. In this situation, Aventail Connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server. Then, based on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed. Page 79:

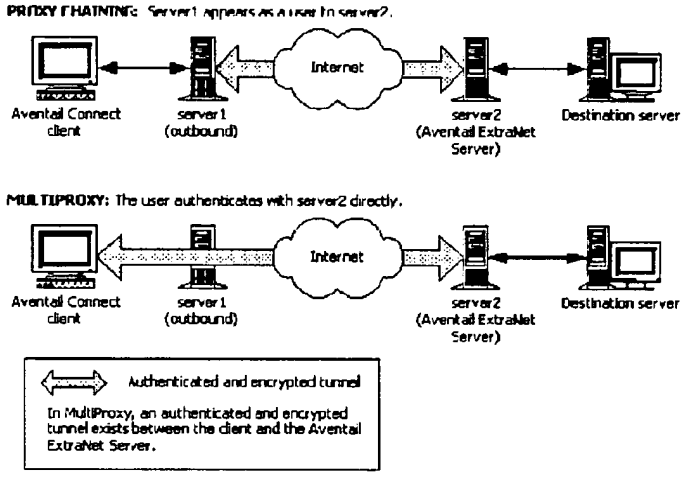
Petitioner Apple Inc. - Exhibit 1002, p. 580

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	 Page 116: Virtual Private Network: A secure channel used to transmit data over a public network.
receiving a secure domain name;	Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname. Page 12: If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet (SOCKS) server in step 2 and the SOCKS server performs the hostname resolution. Page 12: When the connection is completed, Aventail Connect begins the SOCKS negotiation. It sends the list of authentication methods enabled in the configuration file. Once the server selects an authentication method, Aventail Connect executes the specified authentication processing. It then sends the proxy request to the extranet (SOCKS) server. This includes either the IP address provided by the application or the DNS entry (hostname) provided in step 1.

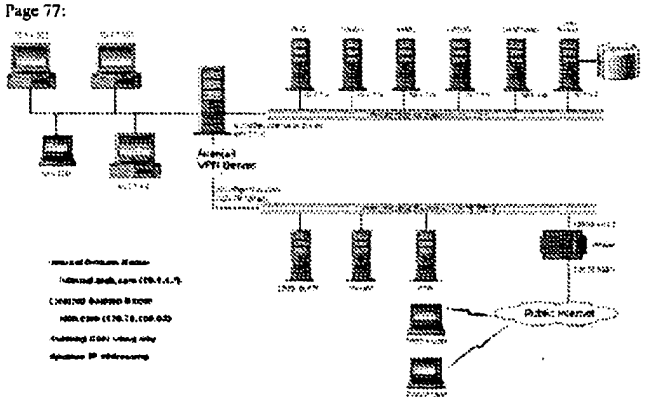
Petitioner Apple Inc. - Exhibit 1002, p. 581

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;	Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname. Page 12: • If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet SOCKS server in step 2 and the SOCKS server performs the hostname resolution. • If the DNS proxy option is enabled and the domain cannot be looked up directly, Aventail Connect creates a false DNS entry that it can recognize later and returns this to the calling application. The false entry tells Aventail Connect that the DNS lookup must be proxied and that it must send the fully qualified hostname to the SOCKS server with the SOCKS connection request. Page 45: Name Resolution instructs Aventail Connect to resolve hostnames locally without needing to venture on to the Internet. This optional feature offers you another level of control over how Aventail Connect performs name resolution. Page 68: The Aventail MultiProxy feature allows Aventail Connect to traverse multiple firewalls by making connections through successive proxy servers. Aventail Connect makes a connection with each proxy server individually. Each proxy server forms a link in a chain that connects Aventail Connect to the final destination. Any or all of the proxy servers can apply authentication and access control rules.
receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and	Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname. Page 12: • If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet SOCKS server in step 2 and the SOCKS server performs the hostname resolution. • If the DNS proxy option is enabled and the domain cannot be looked up directly, Aventail Connect creates a false DNS entry that it can recognize later and returns this to the calling application. The false entry tells Aventail Connect that the DNS lookup must be proxied and that it must send the fully qualified hostname to the SOCKS server with the SOCKS connection request. Page 96: To use Extranet Neighborhood in the static host list mode, you must define, in the hosts file, each individual host in the domain. This allows you to restrict access to designated hosts only. In the hosts file, you must specify the host's IP address or DNS name along with the Windows machine name.
sending an access request message to the secure computer network address using a virtual private network communication link.	Page 6: Escalating security threats are forcing companies to seek ways to safeguard their corporate networks and the information they exchange. . . . Enter SOCKS v5, an Internet Engineering Task Force (IETF)-approved security protocol targeted at securely traversing corporate firewalls. SOCKS was originally developed in 1990, and is now maintained by NEC. SOCKS acts as circuit-level proxy mechanism that manages the flow and security of data traffic to and from your local area network (LAN) or extranet. Page 7: Aventail Connect is designed to run transparently on each workstation, without adding overhead to the users desktop. In most cases users will interact with Aventail Connect only when it prompts them to enter authentication credentials for a connection to a secure extranet (SOCKS) server. Users may also occasionally

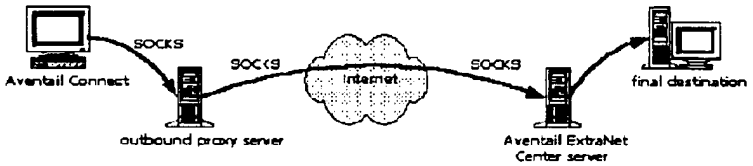
Petitioner Apple Inc. - Exhibit 1002, p. 582

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	need to start and exit Aventail Connect, although network administrators often configure it to run automatically at startup. Aventail Connect does not require administrators to manually establish an encrypted tunnel; Aventail Connect can establish an encrypted tunnel automatically. Page 8: The application requests a connection to the specified remote host. This causes the underlying stack to begin the TCP handshake, when two computers initiate communication with each other. When the handshake is complete, the application is notified that the connection is established, and data can then be transmitted and received. Page 12: If the request contains a real IP address and the configuration file rules say it must be proxied, Aventail Connect will call WinSock to begin the TCP handshake with the server designated in the configuration file. Page 69: The client application requests access to the destination server. Page 72:  Page 77: The Aventail ExtraNet depicted in this example is used to provide secure and monitored access to the

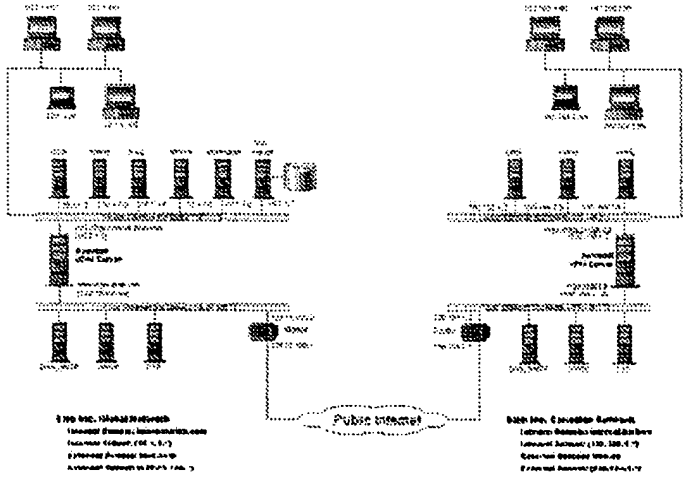
Petitioner Apple Inc. - Exhibit 1002, p. 583

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	private LAN for mobile employees and partners. Page 77: Depending on the security policy and the Aventail ExtraNet Server configuration, Aventail Connect will automatically proxy their allowed application traffic into the private network. In this situation, Aventail Connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server. Then, based on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed. Page 77:  Example Corporate Network Design using Mobile VPN Page 96: To use Extranet Neighborhood in the static host list mode, you must define, in the hosts file, each individual host in the domain. This allows you to restrict access to designated hosts only. In the hosts file, you must specify the host's IP address or DNS name along with the Windows machine name. Page 116: Virtual Private Network: A secure channel used to transmit data over a public network.
4. The method according to claim 1, wherein the response message contains provisioning information for the virtual private network.	Page 68: To gain access to your extranet, users may need to traverse multiple firewalls. In the simplest case, this involves an employee at a partner company gaining access to the Internet via an outbound proxy server at the partner company, and having an authenticated, encrypted, and controlled connection to your internal network via an Aventail ExtraNet Server.

Petitioner Apple Inc. - Exhibit 1002, p. 584

7.188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	The Aventail MultiProxy feature allows Aventail Connect to traverse multiple firewalls by making connections through successive proxy servers. Aventail Connect makes a connection with each proxy server individually. Each proxy server forms a link in a chain that connects Aventail Connect to the final destination. Any or all of the proxy servers can apply authentication and access control rules. Page 69: In the following diagram, the Aventail ExtraNet Server acts as both a destination and a server. It is a destination because a proxy server routes traffic to it. It is a server because it routes traffic to the final destination.  Page 77: Depending on the security policy and the Aventail ExtraNet Server configuration, Aventail Connect will automatically proxy their allowed application traffic into the private network. In this situation, Aventail Connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server. Then, based on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed.
10. The method according to claim 1, wherein the virtual private network includes the Internet.	Page 5: Aventail Corporation is the leading vendor of extranet software. Its extranet solutions allow organizations to secure their networked communications and manage their employees' access to the Internet. Building an extranet gives organizations the ability to dynamically create a private communication or data channel over the Internet. Page 8: Windows TCP/IP networking applications (such as telnet, e-mail, Web browsers, and ftp) use WinSock to gain access to networks or the Internet. WinSock is the core component of TCP/IP under Windows, and is the interface that most Windows applications use to communicate to TCP/IP. Page 79:

Petitioner Apple Inc. - Exhibit 1002, p. 585

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	 Example Corporate Network Design using Partner VPN
12. The method of claim 1, wherein the access request message contains a request for information stored at the secure computer network address.	Page 6: Escalating security threats are forcing companies to seek ways to safeguard their corporate networks and the information they exchange. . . . Enter SOCKS v5, an Internet Engineering Task Force (IETF)-approved security protocol targeted at securely traversing corporate firewalls. SOCKS was originally developed in 1990, and is now maintained by NEC. SOCKS acts as circuit-level proxy mechanism that manages the flow and security of data traffic to and from your local area network (LAN) or extranet. Page 8: The application requests a connection to the specified remote host. This causes the underlying stack to begin the TCP handshake, when two computers initiate communication with each other. When the handshake is complete, the application is notified that the connection is established, and data can then be transmitted and received. Pages 12-13: When the SOCKS negotiation is completed, Aventail Connect notifies the application. From the application's point of view, the entire SOCKS negotiation, including the authentication negotiation, is merely the

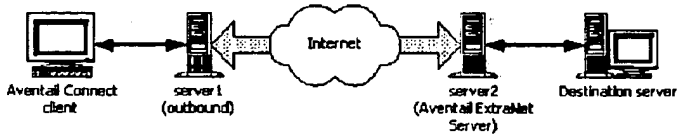
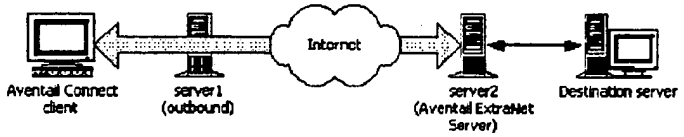
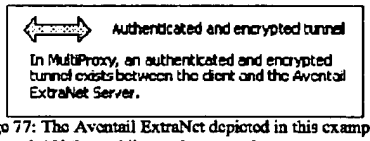
Petitioner Apple Inc. - Exhibit 1002, p. 586

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	TCP handshaking. Page 69: Once the connection between the client and the Aventail ExtraNet Server is established, the output server simply relays the data. Page 69: The client application requests access to the destination server. Page 77: The Aventail ExtraNet depicted in this example is used to provide secure and monitored access to the private LAN for mobile employees and partners.
13. The method of claim 1,	
wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;	Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname. Page 12: If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet (SOCKS) server in step 2 and the SOCKS server performs the hostname resolution. Page 12: When the connection is completed, Aventail Connect begins the SOCKS negotiation. It sends the list of authentication methods enabled in the configuration file. Once the server selects an authentication method, Aventail Connect executes the specified authentication processing. It then sends the proxy request to the extranet (SOCKS) server. This includes either the IP address provided by the application or the DNS entry (hostname) provided in step 1.
wherein sending the query message comprises sending the query message at the client computer;	Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname. Page 12: • If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet SOCKS server in step 2 and the SOCKS server performs the hostname resolution. • If the DNS proxy option is enabled and the domain cannot be looked up directly, Aventail Connect creates a false DNS entry that it can recognize later and returns this to the calling application. The false entry tells Aventail Connect that the DNS lookup must be proxied and that it must send the fully qualified hostname to the SOCKS server with the SOCKS connection request. Page 45: Name Resolution instructs Aventail Connect to resolve hostnames locally without needing to venture on to the Internet. This optional feature offers you another level of control over how Aventail Connect performs name resolution. Page 68: The Aventail MultiProxy feature allows Aventail Connect to traverse multiple firewalls by making connections through successive proxy servers. Aventail Connect makes a connection with each proxy server individually. Each proxy server forms a link in a chain that connects Aventail Connect to the final destination. Any or all of the proxy servers can apply authentication and access control rules.
wherein receiving the response message comprises receiving the response	Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname.

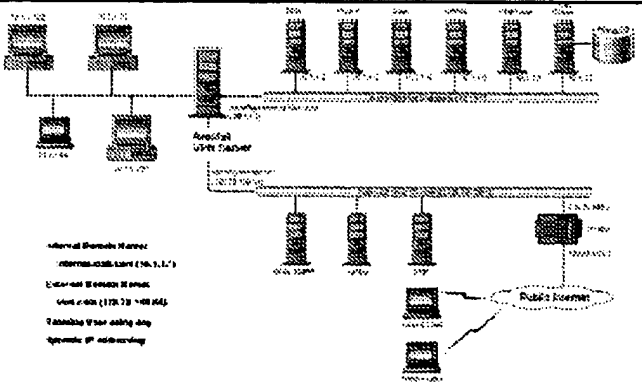
Petitioner Apple Inc. - Exhibit 1002, p. 587

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
message at the client computer,	Page 12: • If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet SOCKS server in step 2 and the SOCKS server performs the hostname resolution. • If the DNS proxy option is enabled and the domain cannot be looked up directly, Aventail Connect creates a false DNS entry that it can recognize later and returns this to the calling application. The false entry tells Aventail Connect that the DNS lookup must be proxied and that it must send the fully qualified hostname to the SOCKS server with the SOCKS connection request. Page 96: To use Extranet Neighborhood in the static host list mode, you must define, in the hosts file, each individual host in the domain. This allows you to restrict access to designated hosts only. In the hosts file, you must specify the host's IP address or DNS name along with the Windows machine name.
wherein sending the access request message comprises sending the access request message at the client computer.	Page 6: Escalating security threats are forcing companies to seek ways to safeguard their corporate networks and the information they exchange. . . . Enter SOCKS v5, an Internet Engineering Task Force (IETF)-approved security protocol targeted at securely traversing corporate firewalls. SOCKS was originally developed in 1990, and is now maintained by NEC. SOCKS acts as circuit-level proxy mechanism that manages the flow and security of data traffic to and from your local area network (LAN) or extranet. Page 7: Aventail Connect is designed to run transparently on each workstation, without adding overhead to the users desktop. In most cases users will interact with Aventail Connect only when it prompts them to enter authentication credentials for a connection to a secure extranet (SOCKS) server. Users may also occasionally need to start and exit Aventail Connect, although network administrators often configure it to run automatically at startup. Aventail Connect does not require administrators to manually establish an encrypted tunnel; Aventail Connect can establish an encrypted tunnel automatically. Page 8: The application requests a connection to the specified remote host. This causes the underlying stack to begin the TCP handshake, when two computers initiate communication with each other. When the handshake is complete, the application is notified that the connection is established, and data can then be transmitted and received. Page 12: If the request contains a real IP address and the configuration file rules say it must be proxied, Aventail Connect will call WinSock to begin the TCP handshake with the server designated in the configuration file. Page 69: The client application requests access to the destination server. Page 72:

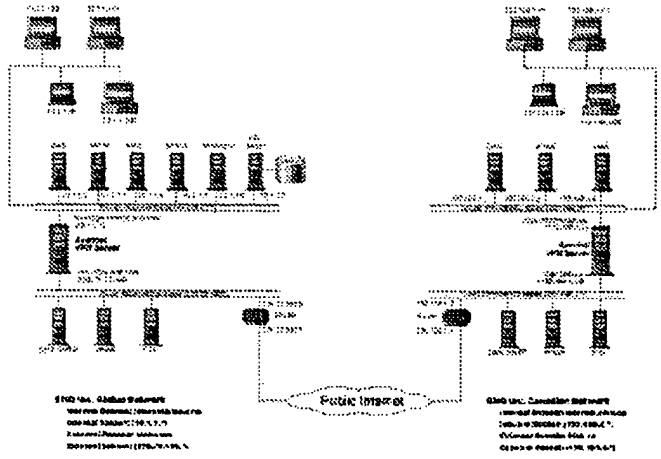
Petitioner Apple Inc. - Exhibit 1002, p. 588

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	PROXY CHAINING: Server1 appears as a user to server2.  **MULTIPROXY:** The user authenticates with server2 directly.   Page 77: The Aventail ExtraNet depicted in this example is used to provide secure and monitored access to the private LAN for mobile employees and partners. Page 77: Depending on the security policy and the Aventail ExtraNet Server configuration, Aventail Connect will automatically proxy their allowed application traffic into the private network. In this situation, Aventail Connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server. Then, based on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed. Page 77:

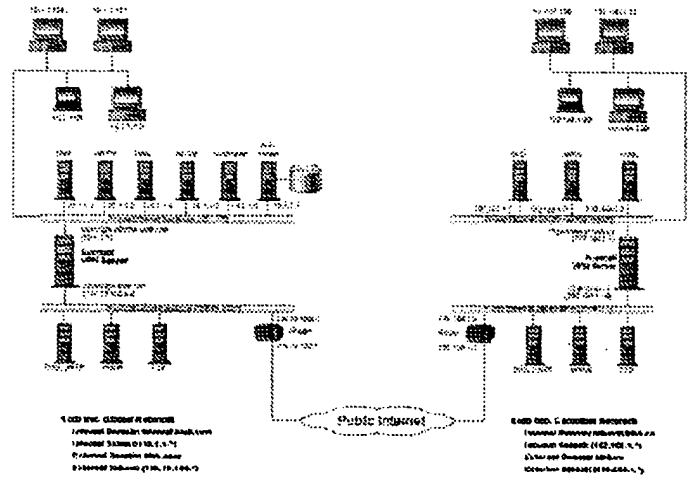
Petitioner Apple Inc. - Exhibit 1002, p. 589

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	 Example Corporate Network Design using Mobile VPN Page 96: To use Extranet Neighborhood in the static host list mode, you must define, in the hosts file, each individual host in the domain. This allows you to restrict access to designated hosts only. In the hosts file, you must specify the host's IP address or DNS name along with the Windows machine name. Page 116: Virtual Private Network: A secure channel used to transmit data over a public network.
14. The method of claim 1, performed by a software module.	*See* claim 1, which is performed by software at the client computer (i.e., Aventail at the client computer).
15. The method of claim 1, performed by a client computer.	*See* claim 1, which is performed by software at the client computer (i.e., Aventail at the client computer). Page 7: Aventail Connect is designed to run transparently on each workstation, without adding overhead to the user's desktop.
17. A computer-readable storage medium, comprising:	Page 14: Regardless of platform, Aventail Connect can be delivered on CD or as a network-delivered, self-extracting archive file. Page 15: After your Aventail ExtraNet Server is set up, Aventail Connect can be installed to single workstation or to multiple networked workstations. In either case, you must perform an initial installation of the software and create one or more configuration (.cfg) files.

Petitioner Apple Inc. - Exhibit 1002, p. 590

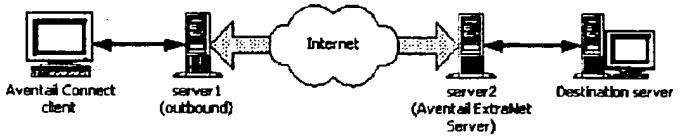
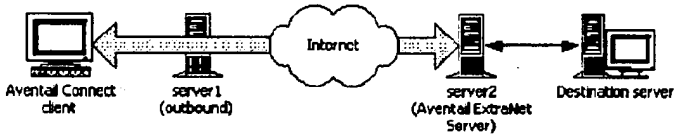
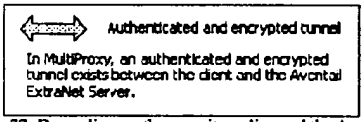
7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	Page 18: In general, the process of installing Aventail Connect to multiple networked workstations involves selecting a file server to use, creating staging area for the Aventail Connect software, and placing the Aventail Connect package in a shared network directory or other publicly accessible location. Page 21: When you load a package, Customizer reads the setup control file to determine what information the package contains. Customizer uses this information to populate the Customizer Editor window. Customizer also reads the configuration file(s) into memory; configuration files are stored in memory to facilitate adding them to and removing them from a package. Page 79:  Example Corporate Network Design using Partner VPN
a storage area; and	Page 14: Regardless of platform, Aventail Connect can be delivered on CD or as a network-delivered, self-extracting archive file. Page 15: After your Aventail ExtraNet Server is set up, Aventail Connect can be installed to single workstation or to multiple networked workstations. In either case, you must perform an initial installation of the software and create one or more configuration (.cfg) files. Page 18: In general, the process of installing Aventail Connect to multiple networked workstations involves

Petitioner Apple Inc. - Exhibit 1002, p. 591

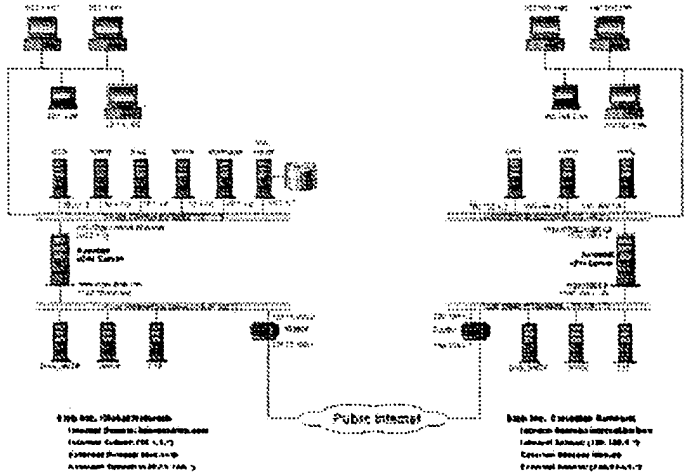
7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	selecting a file server to use, creating staging area for the Aventail Connect software, and placing the Aventail Connect package in a shared network directory or other publicly accessible location. Page 21: When you load a package, Customizer reads the setup control file to determine what information the package contains. Customizer uses this information to populate the Customizer Editor window. Customizer also reads the configuration file(s) into memory; configuration files are stored in memory to facilitate adding them to and removing them from a package. Page 79:  Example Corporate Network Design using Partner VPN
computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:	Page 14: Regardless of platform, Aventail Connect can be delivered on CD or as a network-delivered, self-extracting archive file. Page 6: Escalating security threats are forcing companies to seek ways to safeguard their corporate networks and the information they exchange. The first response to these concerns has been the development of security firewalls—software barriers that control the flow of information. But firewalls are not designed to handle complex security issues, such as monitoring network usage, providing private communication over public

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	networks, and enabling remote users to gain secure access to internal network resources. Page 12: b. When the connection is completed, Aventail Connect begins the SOCKS negotiation. • It sends the list of authentication methods enabled in the configuration file • Once the server selects an authentication method, Aventail Connect executes the specified authentication processing. • It then sends the proxy request to the extranet (SOCKS) server. This includes either the IP address provided by the application or the DNS entry (hostname) provided in step 1. Page 46: SOCKS v5 servers often require user authentication before allowing access. Aventail Connect authentication modules display dialog boxes that prompt users to enter username and password information as well as other authentication credentials. The current Aventail Connect authentication modules are SOCKS v4 Identification, Username / Password, Challenge Handshake Authentication Protocol (CHAP), Challenge Response Authentication Method (CRAM), Secure Sockets Layer (SSL), and HTTP Basic (username/password). Page 62: Once servers and destinations are defined, you can direct SOCKS traffic through successive extranet (SOCKS) servers. Page 66: To gain access to your extranet, users may need to traverse multiple firewalls. In the simplest case, this involves an employee at a partner company gaining access to the Internet via an outbound proxy server at the partner company, and having an authenticated, encrypted, and controlled connection to your internal network via an Aventail ExtraNet Server. This capability is provided in Aventail Connect 3.1 by the Aventail MultiProxy feature. Aventail Connect can open connections through SOCKS servers, through HTTP proxies, or through proxy chaining. Page 72:

Petitioner Apple Inc. - Exhibit 1002, p. 593

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	PROXY CHAINING: Server1 appears as a user to server2.  **MULTIPROXY:** The user authenticates with server2 directly.   Page 77: Depending on the security policy and the Aventail ExtraNet Server configuration, Aventail Connect will automatically proxy their allowed application traffic into the private network. In this situation, Aventail Connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server. Then, based on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed. Page 79:

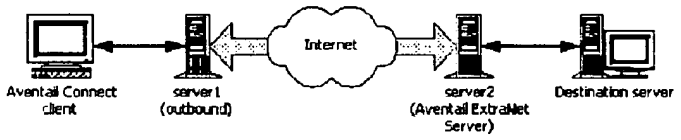
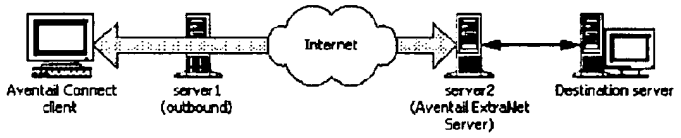
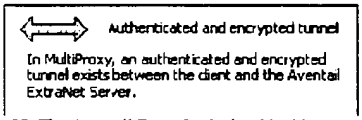
Petitioner Apple Inc. - Exhibit 1002, p. 594

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	 Example Corporate Network Design using Partner VPN Page 116: Virtual Private Network: A secure channel used to transmit data over a public network.
receiving a secure domain name;	Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname. Page 12: If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet (SOCKS) server in step 2 and the SOCKS server performs the hostname resolution. Page 12: When the connection is completed, Aventail Connect begins the SOCKS negotiation. It sends the list of authentication methods enabled in the configuration file. Once the server selects an authentication method, Aventail Connect executes the specified authentication processing. It then sends the proxy request to the extranet (SOCKS) server. This includes either the IP address provided by the application or the DNS entry (hostname) provided in step 1.

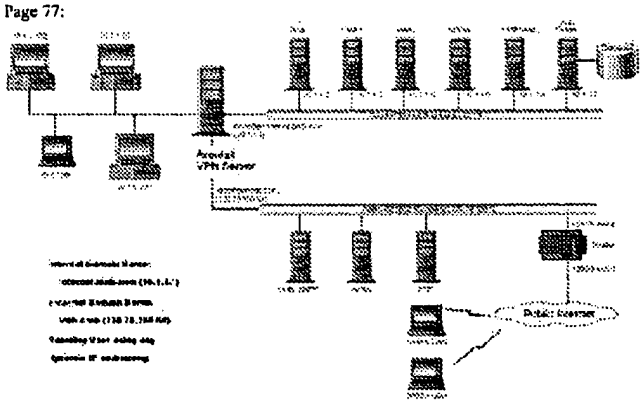
Petitioner Apple Inc. - Exhibit 1002, p. 595

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain name;	Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname. Page 12: • If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet SOCKS server in step 2 and the SOCKS server performs the hostname resolution. • If the DNS proxy option is enabled and the domain cannot be looked up directly, Aventail Connect creates a false DNS entry that it can recognize later and returns this to the calling application. The false entry tells Aventail Connect that the DNS lookup must be proxied and that it must send the fully qualified hostname to the SOCKS server with the SOCKS connection request. Page 45: Name Resolution instructs Aventail Connect to resolve hostnames locally without needing to venture on to the Internet. This optional feature offers you another level of control over how Aventail Connect performs name resolution. Page 68: The Aventail MultiProxy feature allows Aventail Connect to traverse multiple firewalls by making connections through successive proxy servers. Aventail Connect makes a connection with each proxy server individually. Each proxy server forms a link in a chain that connects Aventail Connect to the final destination. Any or all of the proxy servers can apply authentication and access control rules.
receiving from the domain name service a response message containing the secure computer network address corresponding to the secure domain name; and	Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname. Page 12: • If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet SOCKS server in step 2 and the SOCKS server performs the hostname resolution. • If the DNS proxy option is enabled and the domain cannot be looked up directly, Aventail Connect creates a false DNS entry that it can recognize later and returns this to the calling application. The false entry tells Aventail Connect that the DNS lookup must be proxied and that it must send the fully qualified hostname to the SOCKS server with the SOCKS connection request. Page 96: To use Extranet Neighborhood in the static host list mode, you must define, in the hosts file, each individual host in the domain. This allows you to restrict access to designated hosts only. In the hosts file, you must specify the host's IP address or DNS name along with the Windows machine name.
sending an access request message to the secure computer network address using a virtual private network communication link.	Page 6: Escalating security threats are forcing companies to seek ways to safeguard their corporate networks and the information they exchange. . . . Enter SOCKS v5, an Internet Engineering Task Force (IETF)-approved security protocol targeted at securely traversing corporate firewalls. SOCKS was originally developed in 1990, and is now maintained by NEC. SOCKS acts as circuit-level proxy mechanism that manages the flow and security of data traffic to and from your local area network (LAN) or extranet. Page 7: Aventail Connect is designed to run transparently on each workstation, without adding overhead to the users desktop. In most cases users will interact with Aventail Connect only when it prompts them to enter authentication credentials for a connection to a secure extranet (SOCKS) server. Users may also occasionally

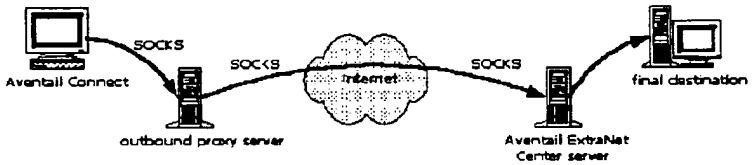
Petitioner Apple Inc. - Exhibit 1002, p. 596

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	need to start and exit Aventail Connect, although network administrators often configure it to run automatically at startup. Aventail Connect does not require administrators to manually establish an encrypted tunnel; Aventail Connect can establish an encrypted tunnel automatically. Page 8: The application requests a connection to the specified remote host. This causes the underlying stack to begin the TCP handshake, when two computers initiate communication with each other. When the handshake is complete, the application is notified that the connection is established, and data can then be transmitted and received. Page 12: If the request contains a real IP address and the configuration file rules say it must be proxied, Aventail Connect will call WinSock to begin the TCP handshake with the server designated in the configuration file. Page 69: The client application requests access to the destination server. Page 72: **PROXY CHAINING:** Server1 appears as a user to server2.  **MULTIPROXY:** The user authenticates with server2 directly.   Page 77: The Aventail ExtraNet depicted in this example is used to provide secure and monitored access to the private LAN for mobile employees and partners. Page 77: Depending on the security policy and the Aventail ExtraNet Server configuration, Aventail Connect will

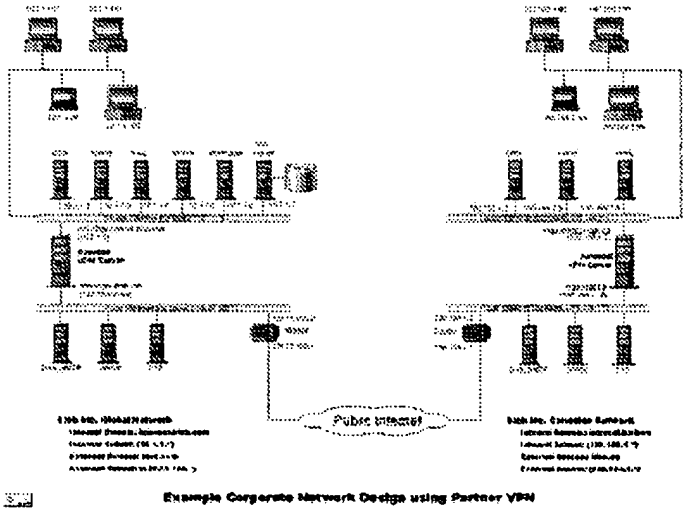
Petitioner Apple Inc. - Exhibit 1002, p. 597

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	automatically proxy their allowed application traffic into the private network. In this situation, Aventail Connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server. Then, based on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed. Page 77:  Example Corporate Network Design using Mobile VPN Page 96: To use Extranet Neighborhood in the static host list mode, you must define, in the hosts file, each individual host in the domain. This allows you to restrict access to designated hosts only. In the hosts file, you must specify the host's IP address or DNS name along with the Windows machine name. Page 116: Virtual Private Network: A secure channel used to transmit data over a public network.
20. The computer-readable medium according to claim 17, wherein the response message contains provisioning information for the virtual private network.	Page 68: To gain access to your extranet, users may need to traverse multiple firewalls. In the simplest case, this involves an employee at a partner company gaining access to the Internet via an outbound proxy server at the partner company, and having an authenticated, encrypted, and controlled connection to your internal network via an Aventail ExtraNet Server. The Aventail MultiProxy feature allows Aventail Connect to traverse multiple firewalls by making connections through successive proxy servers. Aventail Connect makes a connection with each proxy server individually. Each proxy server forms a link in a chain that connects Aventail Connect to the final destination.

Petitioner Apple Inc. - Exhibit 1002, p. 598

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	Any or all of the proxy servers can apply authentication and access control rules. Page 69: In the following diagram, the Aventail ExtraNet Server acts as both a destination and a server. It is a destination because a proxy server routes traffic to it. It is a server because it routes traffic to the final destination.  Page 77: Depending on the security policy and the Aventail ExtraNet Server configuration, Aventail Connect will automatically proxy their allowed application traffic into the private network. In this situation, Aventail Connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server. Then, based on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed.
26. The computer-readable medium according to claim 17, wherein the virtual private network includes the Internet.	Page 5: Aventail Corporation is the leading vendor of extranet software. Its extranet solutions allow organizations to secure their networked communications and manage their employees' access to the Internet. Building an extranet gives organizations the ability to dynamically create a private communication or data channel over the Internet. Page 8: Windows TCP/IP networking applications (such as telnet, e-mail, Web browsers, and ftp) use WinSock to gain access to networks or the Internet. WinSock is the core component of TCP/IP under Windows, and is the interface that most Windows applications use to communicate to TCP/IP. Page 79:

Petitioner Apple Inc. - Exhibit 1002, p. 599

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	 Example Corporate Network Design using Partner VPN
28. The computer readable medium of claim 17, wherein the access request message contains a request for information stored at the secure computer network address.	Page 6: Escalating security threats are forcing companies to seek ways to safeguard their corporate networks and the information they exchange. . . . Enter SOCKS v5, an Internet Engineering Task Force (IETF)-approved security protocol targeted at securely traversing corporate firewalls. SOCKS was originally developed in 1990, and is now maintained by NEC. SOCKS acts as circuit-level proxy mechanism that manages the flow and security of data traffic to and from your local area network (LAN) or extranet. Page 8: The application requests a connection to the specified remote host. This causes the underlying stack to begin the TCP handshake, when two computers initiate communication with each other. When the handshake is complete, the application is notified that the connection is established, and data can then be transmitted and received. Pages 12-13: When the SOCKS negotiation is completed, Aventail Connect notifies the application. From the application's point of view, the entire SOCKS negotiation, including the authentication negotiation, is merely the

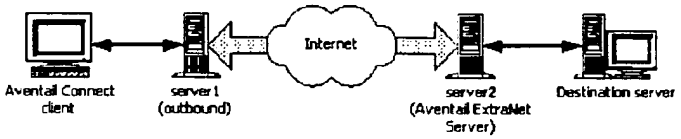
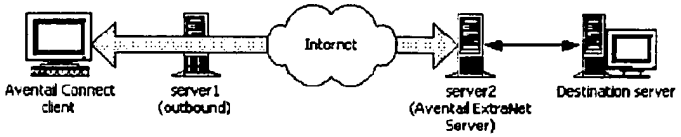
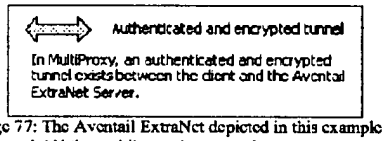
Petitioner Apple Inc. - Exhibit 1002, p. 600

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	TCP handshaking. Page 69: Once the connection between the client and the Aventail ExtraNet Server is established, the output server simply relays the data. Page 69: The client application requests access to the destination server. Page 77: The Aventail ExtraNet depicted in this example is used to provide secure and monitored access to the private LAN for mobile employees and partners.
29. The computer-readable medium according to claim 17,	
wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;	Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname. Page 12: If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet (SOCKS) server in step 2 and the SOCKS server performs the hostname resolution. Page 12: When the connection is completed, Aventail Connect begins the SOCKS negotiation. It sends the list of authentication methods enabled in the configuration file. Once the server selects an authentication method, Aventail Connect executes the specified authentication processing. It then sends the proxy request to the extranet (SOCKS) server. This includes either the IP address provided by the application or the DNS entry (hostname) provided in step 1.
wherein sending the query message comprises sending the query message at the client computer;	Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname. Page 12: • If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet SOCKS server in step 2 and the SOCKS server performs the hostname resolution. • If the DNS proxy option is enabled and the domain cannot be looked up directly, Aventail Connect creates a false DNS entry that it can recognize later and returns this to the calling application. The false entry tells Aventail Connect that the DNS lookup must be proxied and that it must send the fully qualified hostname to the SOCKS server with the SOCKS connection request. Page 45: Name Resolution instructs Aventail Connect to resolve hostnames locally without needing to venture on to the Internet. This optional feature offers you another level of control over how Aventail Connect performs name resolution. Page 68: The Aventail MultiProxy feature allows Aventail Connect to traverse multiple firewalls by making connections through successive proxy servers. Aventail Connect makes a connection with each proxy server individually. Each proxy server forms a link in a chain that connects Aventail Connect to the final destination. Any or all of the proxy servers can apply authentication and access control rules.
wherein receiving the response	Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet

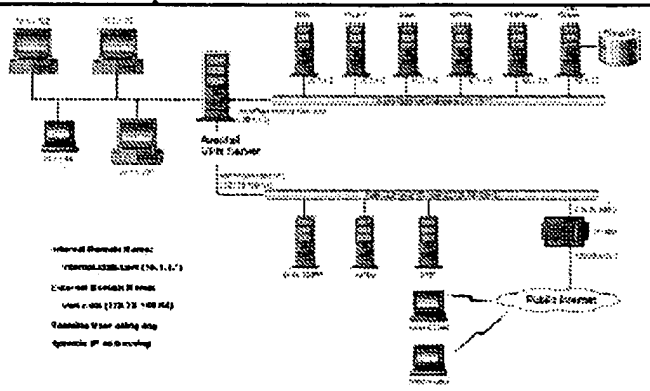
Petitioner Apple Inc. - Exhibit 1002, p. 601

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
message comprises receiving the response message at the client computer,	Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname. Page 12: • If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet SOCKS server in step 2 and the SOCKS server performs the hostname resolution. • If the DNS proxy option is enabled and the domain cannot be looked up directly, Aventail Connect creates a false DNS entry that it can recognize later and returns this to the calling application. The false entry tells Aventail Connect that the DNS lookup must be proxied and that it must send the fully qualified hostname to the SOCKS server with the SOCKS connection request. Page 96: To use Extranet Neighborhood in the static host list mode, you must define, in the hosts file, each individual host in the domain. This allows you to restrict access to designated hosts only. In the hosts file, you must specify the host's IP address or DNS name along with the Windows machine name.
wherein sending the access request message comprises sending the access request message at the client computer.	Page 6: Escalating security threats are forcing companies to seek ways to safeguard their corporate networks and the information they exchange. . . . Enter SOCKS v5, an Internet Engineering Task Force (IETF)-approved security protocol targeted at securely traversing corporate firewalls. SOCKS was originally developed in 1990, and is now maintained by NEC. SOCKS acts as circuit-level proxy mechanism that manages the flow and security of data traffic to and from your local area network (LAN) or extranet. Page 7: Aventail Connect is designed to run transparently on each workstation, without adding overhead to the users desktop. In most cases users will interact with Aventail Connect only when it prompts them to enter authentication credentials for a connection to a secure extranet (SOCKS) server. Users may also occasionally need to start and exit Aventail Connect, although network administrators often configure it to run automatically at startup. Aventail Connect does not require administrators to manually establish an encrypted tunnel; Aventail Connect can establish an encrypted tunnel automatically. Page 8: The application requests a connection to the specified remote host. This causes the underlying stack to begin the TCP handshake, when two computers initiate communication with each other. When the handshake is complete, the application is notified that the connection is established, and data can then be transmitted and received. Page 12: If the request contains a real IP address and the configuration file rules say it must be proxied, Aventail Connect will call WinSock to begin the TCP handshake with the server designated in the configuration file. Page 69: The client application requests access to the destination server. Page 72:

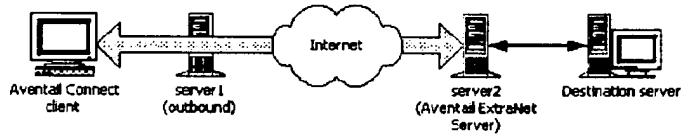
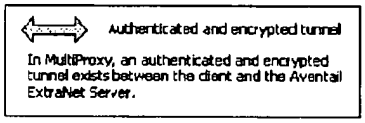
Petitioner Apple Inc. - Exhibit 1002, p. 602

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	PROXY CHAINING: Server1 appears as a user to server2.  **MULTIPROXY:** The user authenticates with server2 directly.   Page 77: The Aventail ExtraNet depicted in this example is used to provide secure and monitored access to the private LAN for mobile employees and partners. Page 77: Depending on the security policy and the Aventail ExtraNet Server configuration, Aventail Connect will automatically proxy their allowed application traffic into the private network. In this situation, Aventail Connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server. Then, based on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed. Page 77:

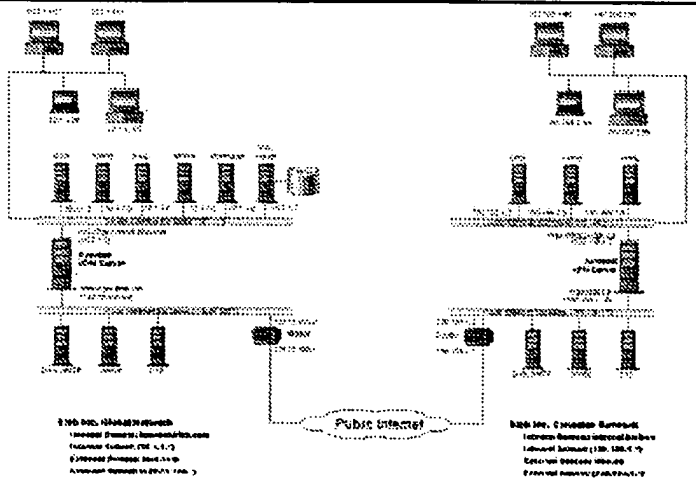
Petitioner Apple Inc. - Exhibit 1002, p. 603

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	 Example Corporate Network Design using Mobile VPN Page 96: To use Extranet Neighborhood in the static host list mode, you must define, in the hosts file, each individual host in the domain. This allows you to restrict access to designated hosts only. In the hosts file, you must specify the host's IP address or DNS name along with the Windows machine name. Page 116: Virtual Private Network: A secure channel used to transmit data over a public network.
30. The computer-readable medium according to claim 17, wherein the method is performed by a software module.	*See* claim 1, which is performed by software at the client computer (i.e., Aventail at the client computer).
31. The computer-readable medium according to claim 17, wherein the method is performed by a client computer.	*See* claim 1, which is performed by software at the client computer (i.e., Aventail at the client computer). Page 7: Aventail Connect is designed to run transparently on each workstation, without adding overhead to the user's desktop.
33. A data processing apparatus, comprising:	Page 15: After your Aventail ExtraNet Server is set up, Aventail Connect can be installed to single workstation or to multiple networked workstations. In either case, you must perform an initial installation of the software and create one or more configuration (.cfg) files.

Petitioner Apple Inc. - Exhibit 1002, p. 604

7.188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	Page 18: In general, the process of installing Aventail Connect to multiple networked workstations involves selecting a file server to use, creating staging area for the Aventail Connect software, and placing the Aventail Connect package in a shared network directory or other publicly accessible location. Page 72: **PROXY CHAINING:** Server1 appears as a user to server2. **MULTIPROXY:** The user authenticates with server2 directly.   Page 79:

Petitioner Apple Inc. - Exhibit 1002, p. 605

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	 Example Corporate Network Design using Partner VPN
a processor, and	Page 13: Aventail Connect Platform Requirements The following table lists the minimum system requirements for each of the platforms that Aventail Connect supports.

Platform	Processor	RAM	SOCKS Server
windows 98; Windows NT 4.0 (requires Microsoft Service Pack 3 or above)	x86-based or Pentium persona. computer	16 MB	Network-accessible SOCKS v4 or v5 compliant server

Petitioner Apple Inc. - Exhibit 1002, p. 606

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference

Windows 95; Windows NT 3.51	x86-based or Pentium personal computer	8 MB	Network-accessible SOCKS v4 or v5 compliant server
Windows 3.1; Windows for Workgroups 3.11	x86-based or Pentium personal computer	4 MB	Network-accessible SOCKS v4 or v5 compliant server

Aventail Connect 3.1 runs on the following operating systems:
Page 15: After your Aventail ExtraNet Server is set up, Aventail Connect can be installed to single workstation or to multiple networked workstations. In either case, you must perform an initial installation of the software and create one or more configuration (.cfg) files.
Page 18: In general, the process of installing Aventail Connect to multiple networked workstations involves selecting a file server to use, creating staging area for the Aventail Connect software, and placing the Aventail Connect package in a shared network directory or other publicly accessible location.
Page 79:

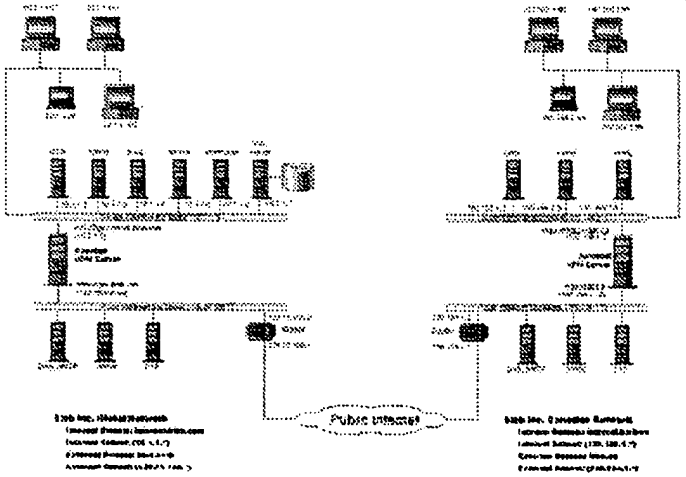
Petitioner Apple Inc. - Exhibit 1002, p. 607

Exhibit B3, Part 5

File History of Reexamination Control No. 95/001,270, reexamination of U.S. 7,188,180 requested by Microsoft Corp.

Customer No.: 000027683

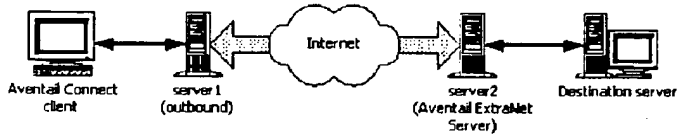
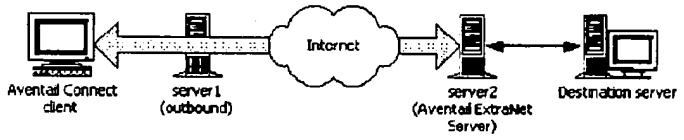
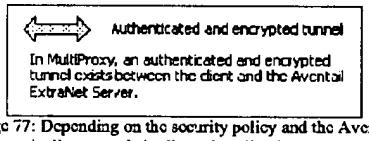
Haynes and Boone, LLP
IP Section
2323 Victory Avenue, Suite 700
Dallas, Texas 75219
Telephone [214] 651.5000
Fax [214] 200.0853

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	 Example Corporate Network Design using Partner VPN
memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:	Page 6: Escalating security threats are forcing companies to seek ways to safeguard their corporate networks and the information they exchange. The first response to these concerns has been the development of security firewalls—software barriers that control the flow of information. But firewalls are not designed to handle complex security issues, such as monitoring network usage, providing private communication over public networks, and enabling remote users to gain secure access to internal network resources. Page 12: b. When the connection is completed, Aventail Connect begins the SOCKS negotiation. • It sends the list of authentication methods enabled in the configuration file • Once the server selects an authentication method, Aventail Connect executes the specified authentication processing. • It then sends the proxy request to the extranet (SOCKS) server. This includes either the IP address

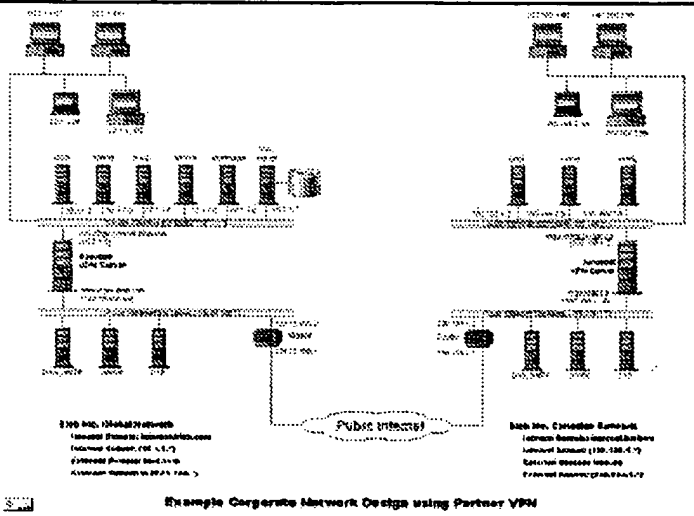
Petitioner Apple Inc. - Exhibit 1002, p. 609

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	provided by the application or the DNS entry (hostname) provided in step 1. Page 46: SOCKS v5 servers often require user authentication before allowing access. Aventail Connect authentication modules display dialog boxes that prompt users to enter username and password information as well as other authentication credentials. The current Aventail Connect authentication modules are SOCKS v4 Identification, Username / Password, Challenge Handshake Authentication Protocol (CHAP), Challenge Response Authentication Method (CRAM), Secure Sockets Layer (SSL), and HTTP Basic (username/password). Page 62: Once servers and destinations are defined, you can direct SOCKS traffic through successive extranet (SOCKS) servers. Page 66: To gain access to your extranet, users may need to traverse multiple firewalls. In the simplest case, this involves an employee at a partner company gaining access to the Internet via an outbound proxy server at the partner company, and having an authenticated, encrypted, and controlled connection to your internal network via an Aventail ExtraNet Server. This capability is provided in Aventail Connect 3.1 by the Aventail MultiProxy feature. Aventail Connect can open connections through SOCKS servers, through HTTP proxies, or through proxy chaining. Page 72:

Petitioner Apple Inc. - Exhibit 1002, p. 610

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	PROXY CHAINING: Server1 appears as a user to server2.  **MULTIPROXY:** The user authenticates with server2 directly.   Page 77: Depending on the security policy and the Aventail ExtraNet Server configuration, Aventail Connect will automatically proxy their allowed application traffic into the private network. In this situation, Aventail Connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server. Then, based on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed. Page 79:

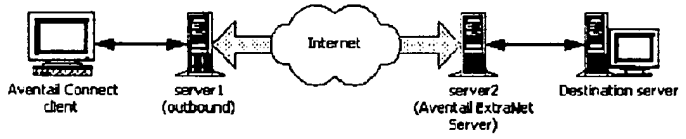
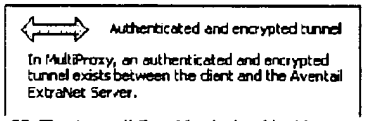
Petitioner Apple Inc. - Exhibit 1002, p. 611

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	 Example Corporate Network Design using Partner VPN Page 116: Virtual Private Network: A secure channel used to transmit data over a public network.
receiving a secure domain name;	Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname. Page 12: If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet (SOCKS) server in step 2 and the SOCKS server performs the hostname resolution. Page 12: When the connection is completed, Aventail Connect begins the SOCKS negotiation. It sends the list of authentication methods enabled in the configuration file. Once the server selects an authentication method, Aventail Connect executes the specified authentication processing. It then sends the proxy request to the extranet (SOCKS) server. This includes either the IP address provided by the application or the DNS entry (hostname) provided in step 1.

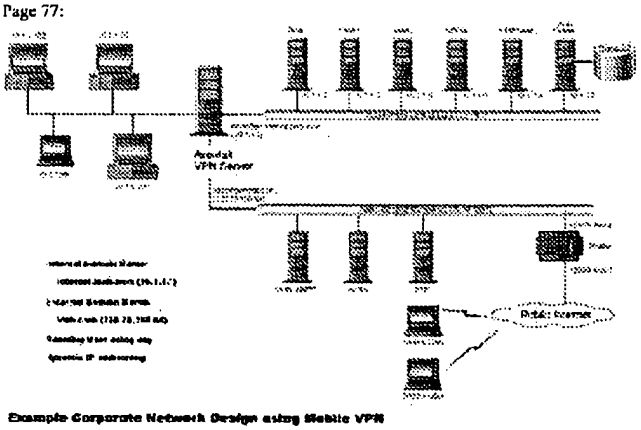
Petitioner Apple Inc. - Exhibit 1002, p. 612

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;	Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname. Page 12: • If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet SOCKS server in step 2 and the SOCKS server performs the hostname resolution. • If the DNS proxy option is enabled and the domain cannot be looked up directly, Aventail Connect creates a false DNS entry that it can recognize later and returns this to the calling application. The false entry tells Aventail Connect that the DNS lookup must be proxied and that it must send the fully qualified hostname to the SOCKS server with the SOCKS connection request. Page 45: Name Resolution instructs Aventail Connect to resolve hostnames locally without needing to venture on to the Internet. This optional feature offers you another level of control over how Aventail Connect performs name resolution. Page 68: The Aventail MultiProxy feature allows Aventail Connect to traverse multiple firewalls by making connections through successive proxy servers. Aventail Connect makes a connection with each proxy server individually. Each proxy server forms a link in a chain that connects Aventail Connect to the final destination. Any or all of the proxy servers can apply authentication and access control rules.
receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and	Page 8: The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname. Page 12: • If the destination hostname matches redirection rule domain name (i.e., the host is part of domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet SOCKS server in step 2 and the SOCKS server performs the hostname resolution. • If the DNS proxy option is enabled and the domain cannot be looked up directly, Aventail Connect creates a false DNS entry that it can recognize later and returns this to the calling application. The false entry tells Aventail Connect that the DNS lookup must be proxied and that it must send the fully qualified hostname to the SOCKS server with the SOCKS connection request. Page 96: To use Extranet Neighborhood in the static host list mode, you must define, in the hosts file, each individual host in the domain. This allows you to restrict access to designated hosts only. In the hosts file, you must specify the host's IP address or DNS name along with the Windows machine name.
sending an access request message to the secure computer network address using a virtual private network communication link.	Page 6: Escalating security threats are forcing companies to seek ways to safeguard their corporate networks and the information they exchange. . . . Enter SOCKS v5, an Internet Engineering Task Force (IETF)-approved security protocol targeted at securely traversing corporate firewalls. SOCKS was originally developed in 1990, and is now maintained by NEC. SOCKS acts as circuit-level proxy mechanism that manages the flow and security of data traffic to and from your local area network (LAN) or extranet. Page 7: Aventail Connect is designed to run transparently on each workstation, without adding overhead to the users desktop. In most cases users will interact with Aventail Connect only when it prompts them to enter authentication credentials for a connection to a secure extranet (SOCKS) server. Users may also occasionally

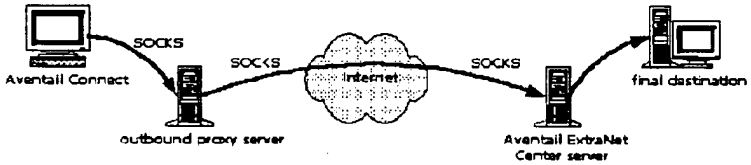
Petitioner Apple Inc. - Exhibit 1002, p. 613

7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	need to start and exit Aventail Connect, although network administrators often configure it to run automatically at startup. Aventail Connect does not require administrators to manually establish an encrypted tunnel; Aventail Connect can establish an encrypted tunnel automatically. Page 8: The application requests a connection to the specified remote host. This causes the underlying stack to begin the TCP handshake, when two computers initiate communication with each other. When the handshake is complete, the application is notified that the connection is established, and data can then be transmitted and received. Page 12: If the request contains a real IP address and the configuration file rules say it must be proxied, Aventail Connect will call WinSock to begin the TCP handshake with the server designated in the configuration file. Page 69: The client application requests access to the destination server. Page 72: **PROXY CHAINING:** Server1 appears as a user to server2.  **MULTIPROXY:** The user authenticates with server2 directly.  Page 77: The Aventail ExtraNet depicted in this example is used to provide secure and monitored access to the private LAN for mobile employees and partners. Page 77: Depending on the security policy and the Aventail ExtraNet Server configuration. Aventail Connect will

Petitioner Apple Inc. - Exhibit 1002, p. 614

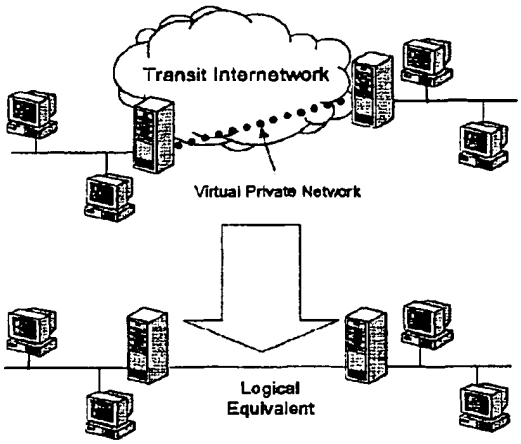
7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	automatically proxy their allowed application traffic into the private network. In this situation, Aventail Connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server. Then, based on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed. Page 77:  Example Corporate Network Design using Mobile VPN Page 96: To use Extranet Neighborhood in the static host list mode, you must define, in the hosts file, each individual host in the domain. This allows you to restrict access to designated hosts only. In the hosts file, you must specify the host's IP address or DNS name along with the Windows machine name. Page 116: Virtual Private Network: A secure channel used to transmit data over a public network.
35. The apparatus of claim 33, wherein the response message contains provisioning information for the virtual private network.	Page 68: To gain access to your extranet, users may need to traverse multiple firewalls. In the simplest case, this involves an employee at a partner company gaining access to the Internet via an outbound proxy server at the partner company, and having an authenticated, encrypted, and controlled connection to your internal network via an Aventail ExtraNet Server. The Aventail MultiProxy feature allows Aventail Connect to traverse multiple firewalls by making connections through successive proxy servers. Aventail Connect makes a connection with each proxy server individually. Each proxy server forms a link in a chain that connects Aventail Connect to the final destination.

Petitioner Apple Inc. - Exhibit 1002, p. 615

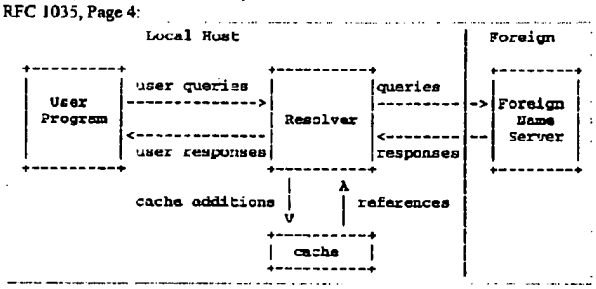
7,188,180 Claim Elements	Description for Claimed Elements in the Aventail Prior Art Reference
	Any or all of the proxy servers can apply authentication and access control rules. Page 69: In the following diagram, the Aventail ExtraNet Server acts as both a destination and a server. It is a destination because a proxy server routes traffic to it. It is a server because it routes traffic to the final destination.  Page 77: Depending on the security policy and the Aventail ExtraNet Server configuration, Aventail Connect will automatically proxy their allowed application traffic into the private network. In this situation, Aventail Connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server. Then, based on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed.

Petitioner Apple Inc. - Exhibit 1002, p. 616

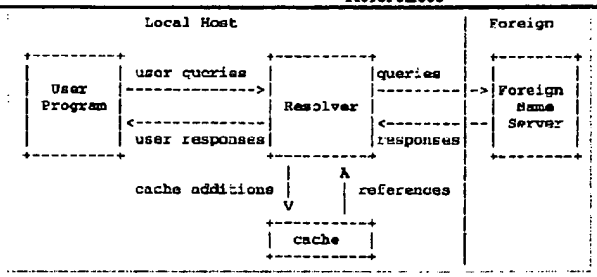
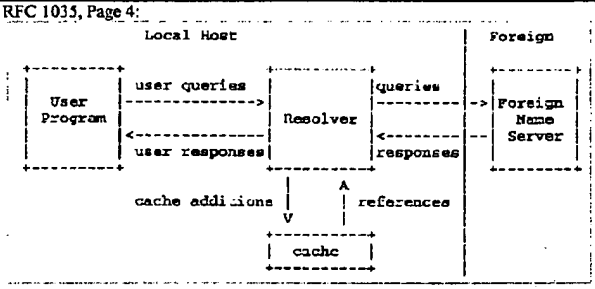
Appendix B
Citations to Exemplary Description in the VPN Overview and RFC 1035 References*

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
1. A method for accessing a secure computer network address, comprising steps of:	VPN Overview, Page 6: A Virtual Private Network (VPN) connects the components of one network over another network. VPNs accomplish this by allowing the user to *tunnel* through the Internet or another public network in a manner that provides the same security and features formerly available only in private networks (see Figure 1).  *Figure 1: Virtual Private Network* VPNs allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet). From the user's perspective, the VPN is a point-to-point connection between the user's computer and a corporate

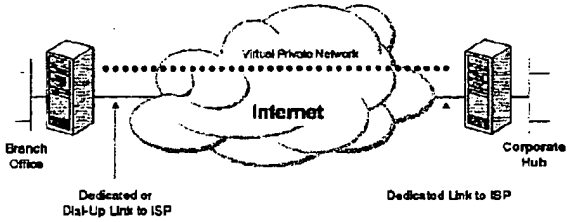
* - The cited passages are an indication of where in the VPN Overview and RFC 1035 references, at the very least, the claims find exemplary description. Requestor reserves the right to identify and demonstrate additional description if necessary or desirable.

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	server. The nature of the intermediate internetwork is irrelevant to the user because it appears as if the data is being sent over a dedicated private link. VPN Overview, Page 9: By using a VPN, the network administrator can ensure that only those users on the corporate internetwork who have appropriate credentials (based on a need-to-know policy within the company) can establish a VPN with the VPN server and gain access to the protected resources of the department. Additionally, all communication across the VPN can be encrypted for data confidentiality. Those users who do not have the proper credentials cannot view the department LAN. User Authentication. The solution must verify the user's identity and restrict VPN access to authorized users only.
receiving a secure domain name;	VPN Overview, Page 26: Redundancy and load balancing is accomplished using round-robin DNS to split requests among a number of VPN tunnel servers that share a common security perimeter. A security perimeter has one external DNS name--for example, vpnx.support.bigcompany.com--but several IP addresses, and loads are randomly distributed across all of the IP addresses. RFC 1035, Page 4: 
sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;	VPN Overview, Page 6: VPNs allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet). VPN Overview, Page 7: VPNs provide remote access to corporate resources over the public Internet, while maintaining privacy of information. RFC 1035, Page 4:

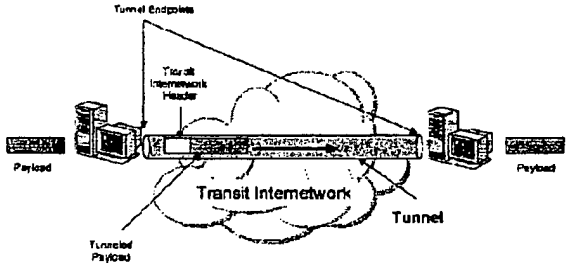
Petitioner Apple Inc. - Exhibit 1002, p. 618

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	
receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and	RFC 1035, Page 4: 
sending an access request message to the secure computer network address using a virtual private network communication link.	VPN Overview, Page 6: VPNs allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet). VPN Overview, Page 7: VPNs provide remote access to corporate resources over the public Internet, while maintaining privacy of information. VPN Overview, Page 8: The VPN software uses the connection to the local ISP to create a virtual private network between the branch office router and the corporate hub router across the Internet.

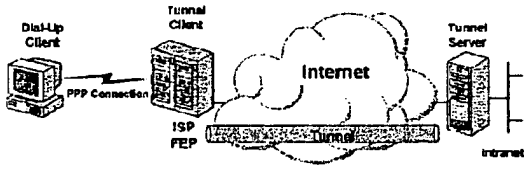
Petitioner Apple Inc. - Exhibit 1002, p. 619

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	 *Figure 3: Using a VPN to connect two remote sites* VPN Overview, Page 9: By using a VPN, the network administrator can ensure that only those users on the corporate internetwork who have appropriate credentials (based on a need-to-know policy within the company) can establish a VPN with the VPN server and gain access to the protected resources of the department. Additionally, all communication across the VPN can be encrypted for data confidentiality. Those users who do not have the proper credentials cannot view the department LAN. User Authentication. The solution must verify the user's identity and restrict VPN access to authorized users only. VPN Overview, Page 10: Tunneling is a method of using an internetwork infrastructure to transfer data for one network over another network. The data to be transferred (or payload) can be the frames (or packets) of another protocol. Instead of sending a frame as it is produced by the originating node, the tunneling protocol encapsulates the frame in an additional header. The additional header provides routing information so that the encapsulated payload can traverse the intermediate internetwork. VPN Overview, Page 10:

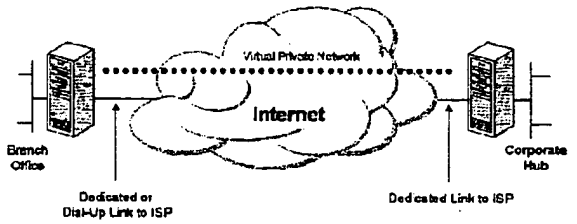
Petitioner Apple Inc. - Exhibit 1002, p. 620

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	 *Figure 5: Tunneling* VPN Overview, Page 12: Once the tunnel is established, tunneled data can be sent. The tunnel client or server uses a tunnel data transfer protocol to prepare the data for transfer. For example, when the tunnel client sends a payload to the tunnel server, the tunnel client first appends a tunnel data transfer protocol header to the payload. The client then sends the resulting encapsulated payload across the internetwork, which routes it to the tunnel server. The tunnel server accepts the packets, removes the tunnel data transfer protocol header, and forwards the payload to the target network. Information sent between the tunnel server and the tunnel client behaves similarly. VPN Overview, Page 12: As a result, any user with access to one of the endpoint machines can use the tunnel. VPN Overview, Page 14: In the second phase, the client PC presents the user's credentials to the remote access server. A secure authentication scheme provides protection against replay attacks and remote client impersonation. VPN Overview, Page 22: This configuration is known as "compulsory" tunneling because the client is compelled to use the tunnel created by the FEP. Once the initial connection is made, all network traffic to and from the client is automatically sent through the tunnel. With compulsory tunneling, the client computer makes a single PPP connection, and when a client dials into the NAS, a tunnel is created and all traffic is automatically routed through the tunnel. VPN Overview, Page 22: In the Internet example, the client computer places a dial-up call to a tunneling-enabled NAS at the ISP. For example, a corporation may have contracted with and ISP to deploy a nationwide set of FEPs. These FEPs can establish tunnels across the Internet to a tunnel server connected to

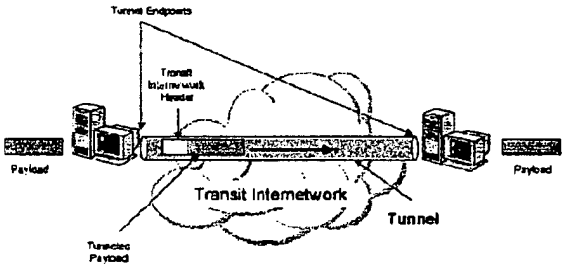
Petitioner Apple Inc. - Exhibit 1002, p. 621

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	the corporation's private network, thereby consolidating calls from geographically diverse locations into a single Internet connection at the corporate network. VPN Overview, Page 22:  *Figure 9: Compulsory tunneling* VPN Overview, Pages 26-27: Redundancy and load balancing is accomplished using round-robin DNS to split requests among a number of VPN tunnel servers that share a common security perimeter. A security perimeter has one external DNS name--for example, vpnx.support.bigcompany.com--but several IP addresses, and loads are randomly distributed across all of the IP addresses. All of the servers can authenticate access requests against a shared database, such as a Windows NT Domain Controller. Note that Windows NT domain databases are replicated by design. VPN Overview, Page 28: As explained in this paper, VPNs allow users or corporations to connect to remote servers, branch offices, or to other companies over a public internetwork, while maintaining secure communications. In all of these cases, the secure connection across appears to the user as a private network communication-despite the fact that this communication occurs over a public internetwork.
4. The method according to claim 1, wherein the response message contains provisioning information for the virtual private network.	VPN Overview, Page 8: The VPN software uses the connection to the local ISP to create a virtual private network between the branch office router and the corporate hub router across the Internet.

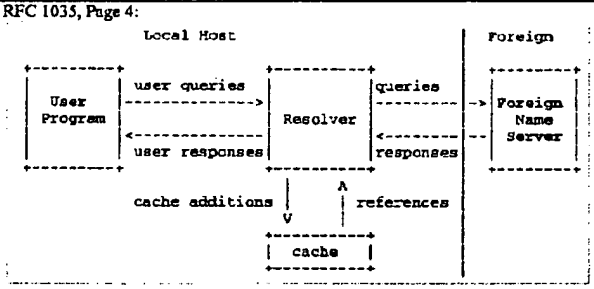
Petitioner Apple Inc. - Exhibit 1002, p. 622

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	 *Figure 3: Using a VPN to connect two remote sites* VPN Overview, Page 9: By using a VPN, the network administrator can ensure that only those users on the corporate internetwork who have appropriate credentials (based on a need-to-know policy within the company) can establish a VPN with the VPN server and gain access to the protected resources of the department. Additionally, all communication across the VPN can be encrypted for data confidentiality. Those users who do not have the proper credentials cannot view the department LAN. User Authentication. The solution must verify the user's identity and restrict VPN access to authorized users only. VPN Overview, Page 12: As a result, any user with access to one of the endpoint machines can use the tunnel. VPN Overview, Page 22: This configuration is known as "compulsory" tunneling because the client is compelled to use the tunnel created by the FEP. Once the initial connection is made, all network traffic to and from the client is automatically sent through the tunnel. With compulsory tunneling, the client computer makes a single PPP connection, and when a client dials into the NAS, a tunnel is created and all traffic is automatically routed through the tunnel. VPN Overview, Pages 26-27: Redundancy and load balancing is accomplished using round-robin DNS to split requests among a number of VPN tunnel servers that share a common security perimeter. A security perimeter has one external DNS name—for example, vpnx.support.bigcompany.com—but several IP addresses, and loads are randomly distributed across all of the IP addresses. All of the servers can authenticate access requests against a shared database, such as a Windows NT Domain Controller. Note that Windows NT domain databases are replicated by design. VPN Overview, Page 28: As explained in this paper, VPNs allow users or corporations to connect to remote servers, branch offices, or to other companies over a public internetwork, while maintaining secure communications. In all of these cases, the secure connection across appears to the user as a private network communication-despite the fact that this communication occurs over a public internetwork.

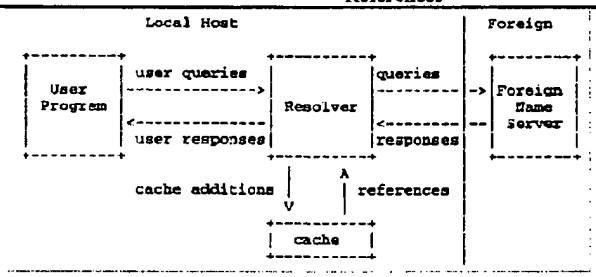
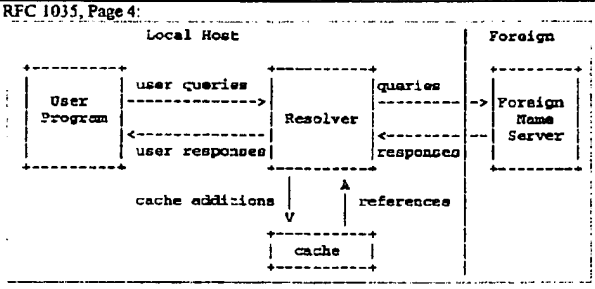
Petitioner Apple Inc. - Exhibit 1002, p. 623

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
10. The method according to claim 1, wherein the virtual private network includes the Internet.	VPN Overview, Page 6: A Virtual Private Network (VPN) connects the components of one network over another network. VPNs accomplish this by allowing the user to *tunnel* through the Internet or another public network in a manner that provides the same security and features formerly available only in private networks (see Figure 1). VPN Overview, Page 10:  *Figure 9: Tunneling*
12. The method of claim 1, wherein the access request message contains a request for information stored at the secure computer network address.	VPN Overview, Page 6: VPNs allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet). VPN Overview, Page 7: VPNs provide remote access to corporate resources over the public Internet, while maintaining privacy of information. VPN Overview, Page 12: Once the tunnel is established, tunneled data can be sent. The tunnel client or server uses a tunnel data transfer protocol to prepare the data for transfer. For example, when the tunnel client sends a payload to the tunnel server, the tunnel client first appends a tunnel data transfer protocol header to the payload. The client then sends the resulting encapsulated payload across the internetwork, which routes it to the tunnel server. The tunnel server accepts the packets, removes the tunnel data transfer protocol header, and forwards the payload to the target network. Information sent between the tunnel server and the tunnel client behaves similarly. VPN Overview, Page 16: Once the four phases of negotiation have been completed, PPP begins to forward

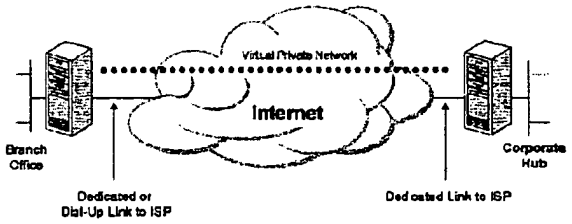
Petitioner Apple Inc. - Exhibit 1002, p. 624

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	data to and from the two peers. VPN Overview, Page 22: This configuration is known as "compulsory" tunneling because the client is compelled to use the tunnel created by the PEP. Once the initial connection is made, all network traffic to and from the client is automatically sent through the tunnel. With compulsory tunneling, the client computer makes a single PPP connection, and when a client dials into the NAS, a tunnel is created and all traffic is automatically routed through the tunnel.
13. The method of claim 1,	
wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;	RFC 1035, Page 4: 
wherein sending the query message comprises sending the query message at the client computer;	RFC 1035, Page 4:

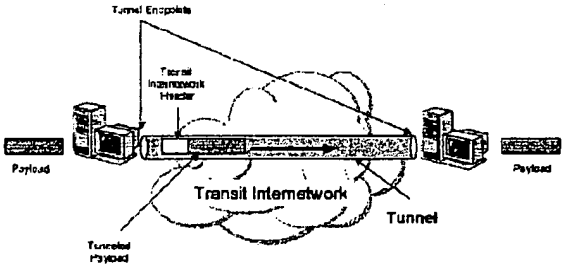
Petitioner Apple Inc. - Exhibit 1002, p. 625

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	
wherein receiving the response message comprises receiving the response message at the client computer,	RFC 1035, Page 4: 
wherein sending the access request message comprises sending the access request message at the client computer.	VPN Overview, Page 6: VPNs allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet). VPN Overview, Page 7: VPNs provide remote access to corporate resources over the public Internet, while maintaining privacy of information. VPN Overview, Page 8: The VPN software uses the connection to the local ISP to create a virtual private network between the branch office router and the corporate hub router across the Internet.

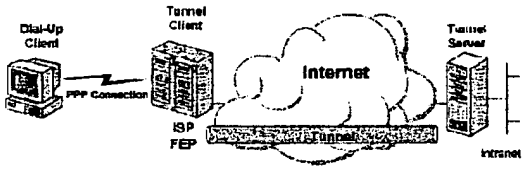
Petitioner Apple Inc. - Exhibit 1002, p. 626

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	 *Figure 3: Using a VPN to connect two remote sites* VPN Overview, Page 9: By using a VPN, the network administrator can ensure that only those users on the corporate internetwork who have appropriate credentials (based on a need-to-know policy within the company) can establish a VPN with the VPN server and gain access to the protected resources of the department. Additionally, all communication across the VPN can be encrypted for data confidentiality. Those users who do not have the proper credentials cannot view the department LAN. User Authentication. The solution must verify the user's identity and restrict VPN access to authorized users only. VPN Overview, Page 10: Tunneling is a method of using an internetwork infrastructure to transfer data for one network over another network. The data to be transferred (or payload) can be the frames (or packets) of another protocol. Instead of sending a frame as it is produced by the originating node, the tunneling protocol encapsulates the frame in an additional header. The additional header provides routing information so that the encapsulated payload can traverse the intermediate internetwork. VPN Overview, Page 10:

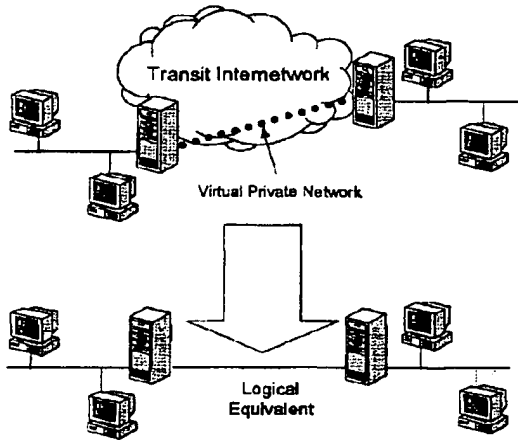
Petitioner Apple Inc. - Exhibit 1002, p. 627

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	 *Figure 6: Tunneling* VPN Overview, Page 12: Once the tunnel is established, tunneled data can be sent. The tunnel client or server uses a tunnel data transfer protocol to prepare the data for transfer. For example, when the tunnel client sends a payload to the tunnel server, the tunnel client first appends a tunnel data transfer protocol header to the payload. The client then sends the resulting encapsulated payload across the internetwork, which routes it to the tunnel server. The tunnel server accepts the packets, removes the tunnel data transfer protocol header, and forwards the payload to the target network. Information sent between the tunnel server and the tunnel client behaves similarly. VPN Overview, Page 12: As a result, any user with access to one of the endpoint machines can use the tunnel. VPN Overview, Page 14: In the second phase, the client PC presents the user's credentials to the remote access server. A secure authentication scheme provides protection against replay attacks and remote client impersonation. VPN Overview, Page 22: This configuration is known as "compulsory" tunneling because the client is compelled to use the tunnel created by the FEP. Once the initial connection is made, all network traffic to and from the client is automatically sent through the tunnel. With compulsory tunneling, the client computer makes a single PPP connection, and when a client dials into the NAS, a tunnel is created and all traffic is automatically routed through the tunnel. VPN Overview, Page 22: In the Internet example, the client computer places a dial-up call to a tunneling-enabled NAS at the ISP. For example, a corporation may have contracted with and ISP to deploy a nationwide set of FEPs. These FEPs can establish tunnels across the Internet to a tunnel server connected to the corporation's private network, thereby consolidating calls from geographically diverse locations into a

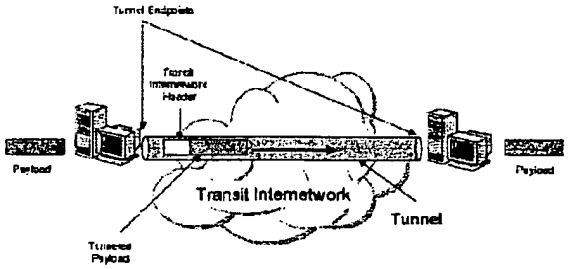
Petitioner Apple Inc. - Exhibit 1002, p. 628

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	single Internet connection at the corporate network. VPN Overview, Page 22:  *Figure 9: Compulsory tunneling* VPN Overview, Pages 26-27: Redundancy and load balancing is accomplished using round-robin DNS to split requests among a number of VPN tunnel servers that share a common security perimeter. A security perimeter has one external DNS name--for example, vpnx.support.bigcompany.com--but several IP addresses, and loads are randomly distributed across all of the IP addresses. All of the servers can authenticate access requests against a shared database, such as a Windows NT Domain Controller. Note that Windows NT domain databases are replicated by design. VPN Overview, Page 28: As explained in this paper, VPNs allow users or corporations to connect to remote servers, branch offices, or to other companies over a public internetwork, while maintaining secure communications. In all of these cases, the secure connection across appears to the user as a private network communication-despite the fact that this communication occurs over a public internetwork.
14. The method of claim 1, performed by a software module.	See claim 1, which is performed by software (Windows NT 4.0) at the client computer.
15. The method of claim 1, performed by a client computer.	See claim 1, which is performed by software (Windows NT 4.0) at the client computer. VPN Overview, Page 6: A Virtual Private Network (VPN) connects the components of one network over another network. VPNs accomplish this by allowing the user to *tunnel* through the Internet or another public network in a manner that provides the same security and features formerly available only in private networks (see Figure 1).

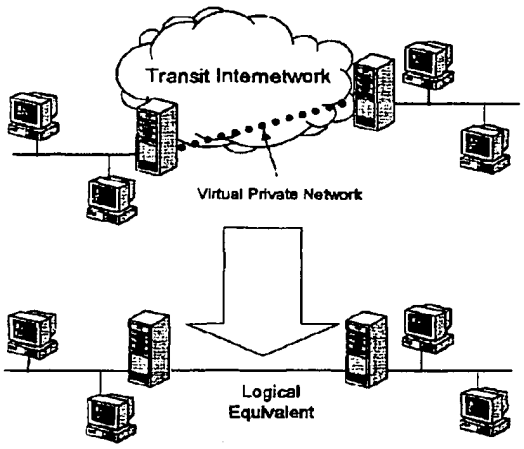
Petitioner Apple Inc. - Exhibit 1002, p. 629

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	 *Figure 1: Virtual Private Network* VPNs allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet). From the user's perspective, the VPN is a point-to-point connection between the user's computer and a corporate server. The nature of the intermediate internetwork is irrelevant to the user because it appears as if the data is being sent over a dedicated private link.
17. A computer-readable storage medium, comprising:	VPN Overview, Page 10:

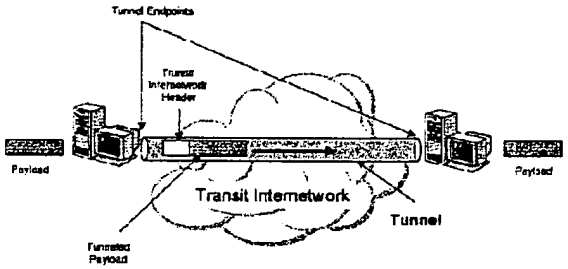
Petitioner Apple Inc. - Exhibit 1002, p. 630

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	 *Figure 6: Tunneling* VPN Overview, Page 21: Voluntary tunneling occurs when a workstation or routing server uses tunneling client software to create a virtual connection to the target tunnel server.
a storage area; and	VPN Overview, Page 21: Voluntary tunneling occurs when a workstation or routing server uses tunneling client software to create a virtual connection to the target tunnel server.
computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:	VPN Overview, Page 6: A Virtual Private Network (VPN) connects the components of one network over another network. VPNs accomplish this by allowing the user to *tunnel* through the Internet or another public network in a manner that provides the same security and features formerly available only in private networks (see Figure 1).

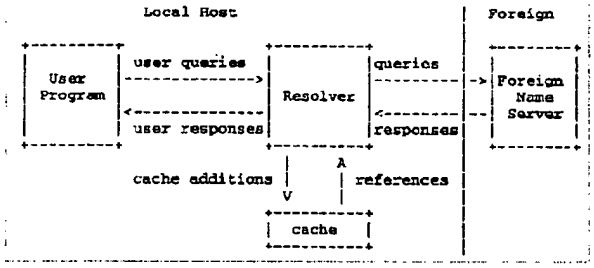
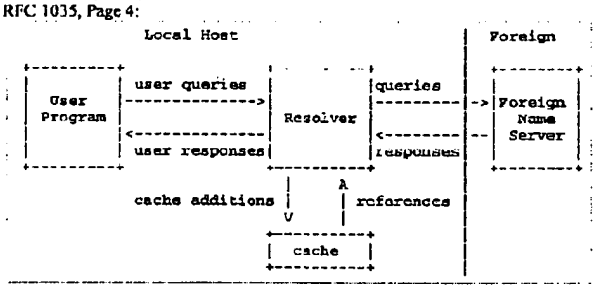
Petitioner Apple Inc. - Exhibit 1002, p. 631

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	 *Figure 1: Virtual Private Network* VPNs allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet). From the user's perspective, the VPN is a point-to-point connection between the user's computer and a corporate server. The nature of the intermediate internetwork is irrelevant to the user because it appears as if the data is being sent over a dedicated private link. VPN Overview, Page 9: By using a VPN, the network administrator can ensure that only those users on the corporate internetwork who have appropriate credentials (based on a need-to-know policy within the company) can establish a VPN with the VPN server and gain access to the protected resources of the department. Additionally, all communication across the VPN can be encrypted for data confidentiality. Those users who do not have the proper credentials cannot view the department LAN. User Authentication. The solution must verify the user's identity and restrict VPN access to authorized

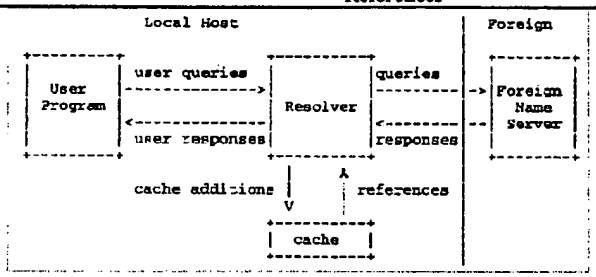
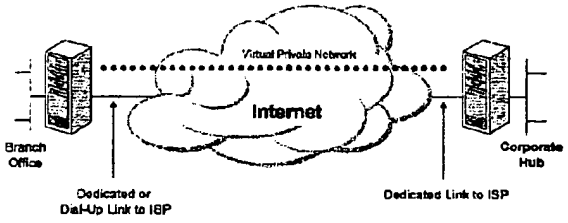
Petitioner Apple Inc. - Exhibit 1002, p. 632

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	users only. VPN Overview, Page 10:  *Figure 6: Tunneling* VPN Overview, Page 21: Voluntary tunneling occurs when a workstation or routing server uses tunneling client software to create a virtual connection to the target tunnel server.
receiving a secure domain name;	VPN Overview, Page 26: Redundancy and load balancing is accomplished using round-robin DNS to split requests among a number of VPN tunnel servers that share a common security perimeter. A security perimeter has one external DNS name--for example, vpnx.support.bigcompany.com--but several IP addresses, and loads are randomly distributed across all of the IP addresses. RFC 1035, Page 4:

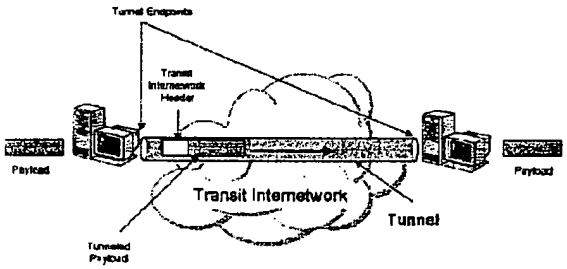
Petitioner Apple Inc. - Exhibit 1002, p. 633

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	
sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain name;	VPN Overview, Page 6: VPNs allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet). VPN Overview, Page 7: VPNs provide remote access to corporate resources over the public Internet, while maintaining privacy of information. RFC 1035, Page 4: 
receiving from the domain name service a response message containing the secure computer network address	RFC 1035, Page 4:

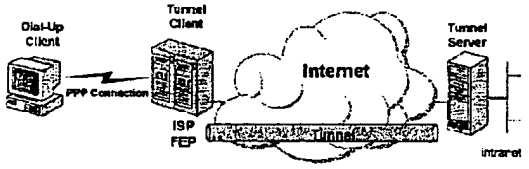
Petitioner Apple Inc. - Exhibit 1002, p. 634

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
corresponding to the secure domain name; and	
sending an access request message to the secure computer network address using a virtual private network communication link.	VPN Overview, Page 6: VPNs allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet). VPN Overview, Page 7: VPNs provide remote access to corporate resources over the public Internet, while maintaining privacy of information. VPN Overview, Page 8: The VPN software uses the connection to the local ISP to create a virtual private network between the branch office router and the corporate hub router across the Internet.  *Figure 3: Using a VPN to connect two remote sites* VPN Overview, Page 9: By using a VPN, the network administrator can ensure that only those users on the corporate internetwork who have appropriate credentials (based on a need-to-know policy within the company) can establish a VPN with the VPN server and gain access to the protected resources of the

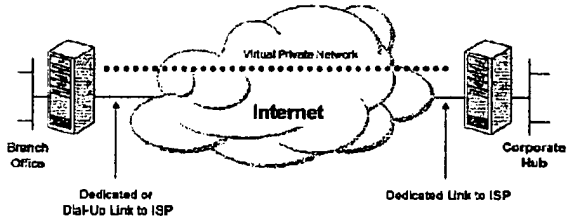
Petitioner Apple Inc. - Exhibit 1002, p. 635

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	department. Additionally, all communication across the VPN can be encrypted for data confidentiality. Those users who do not have the proper credentials cannot view the department LAN. User Authentication. The solution must verify the user's identity and restrict VPN access to authorized users only. VPN Overview, Page 10: Tunneling is a method of using an internetwork infrastructure to transfer data for one network over another network. The data to be transferred (or payload) can be the frames (or packets) of another protocol. Instead of sending a frame as it is produced by the originating node, the tunneling protocol encapsulates the frame in an additional header. The additional header provides routing information so that the encapsulated payload can traverse the intermediate internetwork. VPN Overview, Page 10:  *Figure 5: Tunneling* VPN Overview, Page 12: Once the tunnel is established, tunneled data can be sent. The tunnel client or server uses a tunnel data transfer protocol to prepare the data for transfer. For example, when the tunnel client sends a payload to the tunnel server, the tunnel client first appends a tunnel data transfer protocol header to the payload. The client then sends the resulting encapsulated payload across the internetwork, which routes it to the tunnel server. The tunnel server accepts the packets, removes the tunnel data transfer protocol header, and forwards the payload to the target network. Information sent between the tunnel server and the tunnel client behaves similarly. VPN Overview, Page 12: As a result, any user with access to one of the endpoint machines can use the tunnel. VPN Overview, Page 14: In the second phase, the client PC presents the user's credentials to the remote

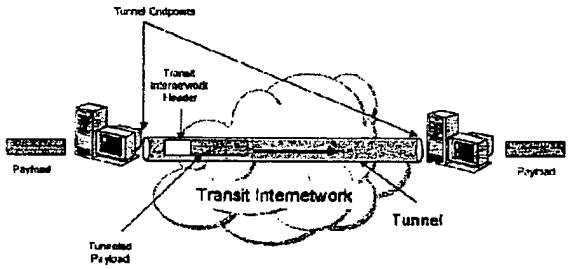
Petitioner Apple Inc. - Exhibit 1002, p. 636

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	access server. A secure authentication scheme provides protection against replay attacks and remote client impersonation. VPN Overview, Page 22: This configuration is known as "compulsory" tunneling because the client is compelled to use the tunnel created by the FEP. Once the initial connection is made, all network traffic to and from the client is automatically sent through the tunnel. With compulsory tunneling, the client computer makes a single PPP connection, and when a client dials into the NAS, a tunnel is created and all traffic is automatically routed through the tunnel. VPN Overview, Page 22: In the Internet example, the client computer places a dial-up call to a tunneling-enabled NAS at the ISP. For example, a corporation may have contracted with and ISP to deploy a nationwide set of FEPs. These FEPs can establish tunnels across the Internet to a tunnel server connected to the corporation's private network, thereby consolidating calls from geographically diverse locations into a single Internet connection at the corporate network. VPN Overview, Page 22:  *Figure 9: Compulsory tunneling* VPN Overview, Pages 26-27: Redundancy and load balancing is accomplished using round-robin DNS to split requests among a number of VPN tunnel servers that share a common security perimeter. A security perimeter has one external DNS name--for example, vpnx.support.bigcompany.com--but several IP addresses, and loads are randomly distributed across all of the IP addresses. All of the servers can authenticate access requests against a shared database, such as a Windows NT Domain Controller. Note that Windows NT domain databases are replicated by design. VPN Overview, Page 28: As explained in this paper, VPNs allow users or corporations to connect to remote servers, branch offices, or to other companies over a public internetwork, while maintaining secure communications. In all of these cases, the secure connection across appears to the user as a private network communication-despite the fact that this communication occurs over a public internetwork.
20. The computer-readable medium	VPN Overview, Page 8: The VPN software uses the connection to the local ISP to create a virtual private

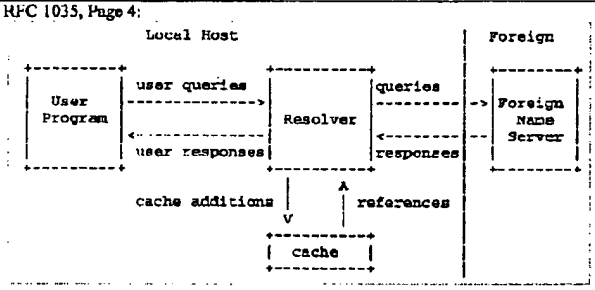
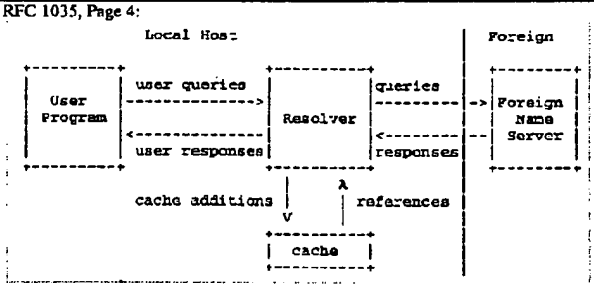
Petitioner Apple Inc. - Exhibit 1002, p. 637

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
according to claim 17, wherein the response message contains provisioning information for the virtual private network.	network between the branch office router and the corporate hub router across the Internet.  *Figure 3: Using a VPN to connect two remote sites* VPN Overview, Page 9: By using a VPN, the network administrator can ensure that only those users on the corporate internetwork who have appropriate credentials (based on a need-to-know policy within the company) can establish a VPN with the VPN server and gain access to the protected resources of the department. Additionally, all communication across the VPN can be encrypted for data confidentiality. Those users who do not have the proper credentials cannot view the department LAN. User Authentication. The solution must verify the user's identity and restrict VPN access to authorized users only. VPN Overview, Page 12: As a result, any user with access to one of the endpoint machines can use the tunnel. VPN Overview, Page 22: This configuration is known as "compulsory" tunneling because the client is compelled to use the tunnel created by the FEP. Once the initial connection is made, all network traffic to and from the client is automatically sent through the tunnel. With compulsory tunneling, the client computer makes a single PPP connection, and when a client dials into the NAS, a tunnel is created and all traffic is automatically routed through the tunnel. VPN Overview, Pages 26-27: Redundancy and load balancing is accomplished using round-robin DNS to split requests among a number of VPN tunnel servers that share a common security perimeter. A security perimeter has one external DNS name--for example, vpnx.support.bigcompany.com--but several IP addresses, and loads are randomly distributed across all of the IP addresses. All of the servers can authenticate access requests against a shared database, such as a Windows NT Domain Controller. Note that Windows NT domain databases are replicated by design. VPN Overview, Page 28: As explained in this paper, VPNs allow users or corporations to connect to remote servers, branch offices, or to other companies over a public internetwork, while maintaining secure communications. In all of these cases, the secure connection across appears to the user as a private network

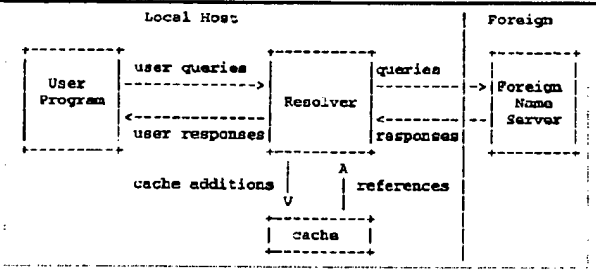
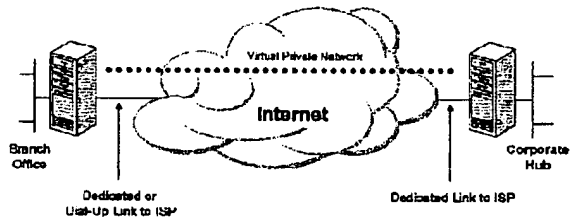
Petitioner Apple Inc. - Exhibit 1002, p. 638

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	communication-despite the fact that this communication occurs over a public internetwork.
26. The computer-readable medium according to claim 17, wherein the virtual private network includes the Internet.	VPN Overview, Page 6: A Virtual Private Network (VPN) connects the components of one network over another network. VPNs accomplish this by allowing the user to *tunnel* through the Internet or another public network in a manner that provides the same security and features formerly available only in private networks (see Figure 1). VPN Overview, Page 10:  *Figure 5: Tunneling*
28. The computer readable medium of claim 17, wherein the access request message contains a request for information stored at the secure computer network address.	VPN Overview, Page 12: Once the tunnel is established, tunneled data can be sent. The tunnel client or server uses a tunnel data transfer protocol to prepare the data for transfer. For example, when the tunnel client sends a payload to the tunnel server, the tunnel client first appends a tunnel data transfer protocol header to the payload. The client then sends the resulting encapsulated payload across the internetwork, which routes it to the tunnel server. The tunnel server accepts the packets, removes the tunnel data transfer protocol header, and forwards the payload to the target network. Information sent between the tunnel server and the tunnel client behaves similarly. VPN Overview, Page 16: Once the four phases of negotiation have been completed, PPP begins to forward data to and from the two peers. VPN Overview, Page 22: This configuration is known as "compulsory" tunneling because the client is compelled to use the tunnel created by the PEP. Once the initial connection is made, all network traffic to and from the client is automatically sent through the tunnel. With compulsory tunneling, the client computer

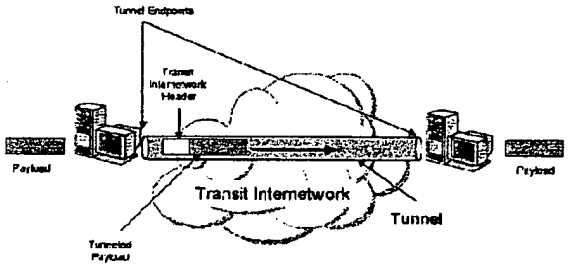
Petitioner Apple Inc. - Exhibit 1002, p. 639

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	makes a single PPP connection, and when a client dials into the NAS, a tunnel is created and all traffic is automatically routed through the tunnel.
29. The computer-readable medium according to claim 17.	
wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;	RFC 1035, Page 4: 
wherein sending the query message comprises sending the query message at the client computer;	RFC 1035, Page 4: 
wherein receiving the response	RFC 1035, Page 4:

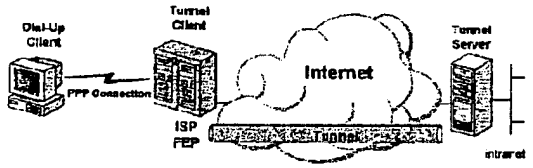
Petitioner Apple Inc. - Exhibit 1002, p. 640

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
message comprises receiving the response message at the client computer,	
wherein sending the access request message comprises sending the access request message at the client computer.	VPN Overview, Page 6: VPNs allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet). VPN Overview, Page 7: VPNs provide remote access to corporate resources over the public Internet, while maintaining privacy of information. VPN Overview, Page 8: The VPN software uses the connection to the local ISP to create a virtual private network between the branch office router and the corporate hub router across the Internet.  *Figure 3: Using a VPN to connect two remote sites* VPN Overview, Page 9: By using a VPN, the network administrator can ensure that only those users on the

Petitioner Apple Inc. - Exhibit 1002, p. 641

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	corporate internetwork who have appropriate credentials (based on a need-to-know policy within the company) can establish a VPN with the VPN server and gain access to the protected resources of the department. Additionally, all communication across the VPN can be encrypted for data confidentiality. Those users who do not have the proper credentials cannot view the department LAN. User Authentication. The solution must verify the user's identity and restrict VPN access to authorized users only. VPN Overview, Page 10: Tunneling is a method of using an internetwork infrastructure to transfer data for one network over another network. The data to be transferred (or payload) can be the frames (or packets) of another protocol. Instead of sending a frame as it is produced by the originating node, the tunneling protocol encapsulates the frame in an additional header. The additional header provides routing information so that the encapsulated payload can traverse the intermediate internetwork. VPN Overview, Page 10:  *Figure 5: Tunneling* VPN Overview, Page 12: Once the tunnel is established, tunneled data can be sent. The tunnel client or server uses a tunnel data transfer protocol to prepare the data for transfer. For example, when the tunnel client sends a payload to the tunnel server, the tunnel client first appends a tunnel data transfer protocol header to the payload. The client then sends the resulting encapsulated payload across the internetwork, which routes it to the tunnel server. The tunnel server accepts the packets, removes the tunnel data transfer protocol header, and forwards the payload to the target network. Information sent between the tunnel server and the tunnel client behaves similarly.

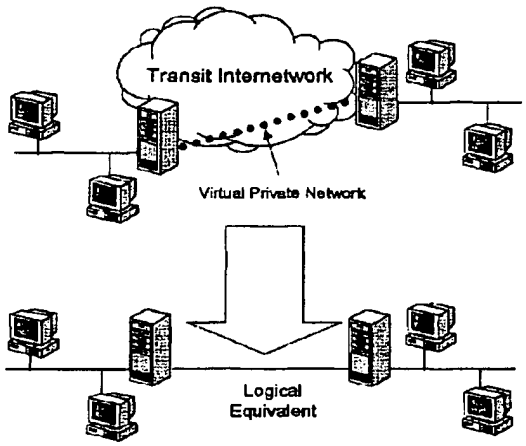
Petitioner Apple Inc. - Exhibit 1002, p. 642

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	VPN Overview, Page 12: As a result, any user with access to one of the endpoint machines can use the tunnel. VPN Overview, Page 14: In the second phase, the client PC presents the user's credentials to the remote access server. A secure authentication scheme provides protection against replay attacks and remote client impersonation. VPN Overview, Page 22: This configuration is known as "compulsory" tunneling because the client is compelled to use the tunnel created by the FEP. Once the initial connection is made, all network traffic to and from the client is automatically sent through the tunnel. With compulsory tunneling, the client computer makes a single PPP connection, and when a client dials into the NAS, a tunnel is created and all traffic is automatically routed through the tunnel. VPN Overview, Page 22: In the Internet example, the client computer places a dial-up call to a tunneling-enabled NAS at the ISP. For example, a corporation may have contracted with and ISP to deploy a nationwide set of FEPs. These FEPs can establish tunnels across the Internet to a tunnel server connected to the corporation's private network, thereby consolidating calls from geographically diverse locations into a single Internet connection at the corporate network. VPN Overview, Page 22:  *Figure 9: Compulsory tunneling* VPN Overview, Pages 26-27: Redundancy and load balancing is accomplished using round-robin DNS to split requests among a number of VPN tunnel servers that share a common security perimeter. A security perimeter has one external DNS name--for example, vpnx.support.bigcompany.com--but several IP addresses, and loads are randomly distributed across all of the IP addresses. All of the servers can authenticate access requests against a shared database, such as a Windows NT Domain Controller. Note that Windows NT domain databases are replicated by design. VPN Overview, Page 28: As explained in this paper, VPNs allow users or corporations to connect to remote servers, branch offices, or to other companies over a public internetwork, while maintaining secure communications. In all of these cases, the secure connection across appears to the user as a private network

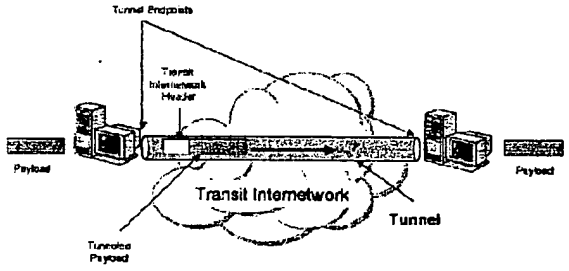
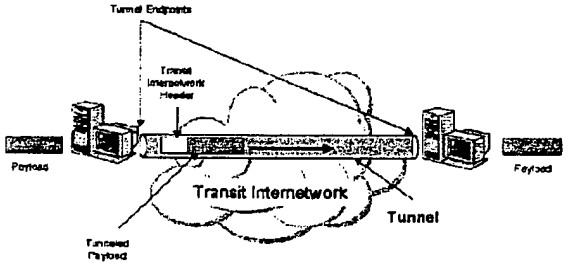
Petitioner Apple Inc. - Exhibit 1002, p. 643

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	communication-despite the fact that this communication occurs over a public internetwork.
30. The computer-readable medium according to claim 17, wherein the method is performed by a software module.	See claim 1, which is performed by software (Windows NT 4.0) at the client computer.
31. The computer-readable medium according to claim 17, wherein the method is performed by a client computer.	See claim 1, which is performed by software (Windows NT 4.0) at the client computer. VPN Overview, Page 6: A Virtual Private Network (VPN) connects the components of one network over another network. VPNs accomplish this by allowing the user to *tunnel* through the Internet or another public network in a manner that provides the same security and features formerly available only in private networks (see Figure 1).

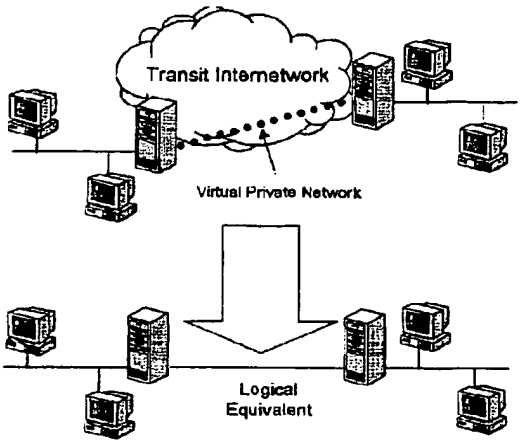
Petitioner Apple Inc. - Exhibit 1002, p. 644

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	 *Figure 1: Virtual Private Network* VPNs allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet). From the user's perspective, the VPN is a point-to-point connection between the user's computer and a corporate server. The nature of the intermediate internetwork is irrelevant to the user because it appears as if the data is being sent over a dedicated private link.
33. A data processing apparatus, comprising:	VPN Overview, Page 10:

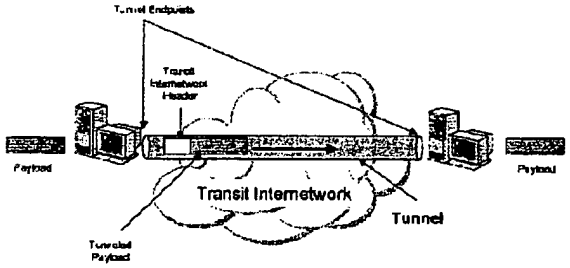
Petitioner Apple Inc. - Exhibit 1002, p. 645

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	 *Figure 6: Tunneling* VPN Overview, Page 21: Voluntary tunneling occurs when a workstation or routing server uses tunneling client software to create a virtual connection to the target tunnel server.
a processor, and	VPN Overview, Page 10:  *Figure 5: Tunneling* VPN Overview, Page 21: Voluntary tunneling occurs when a workstation or routing server uses tunneling client software to create a virtual connection to the target tunnel server.
memory storing computer executable	VPN Overview, Page 6: A Virtual Private Network (VPN) connects the components of one network over

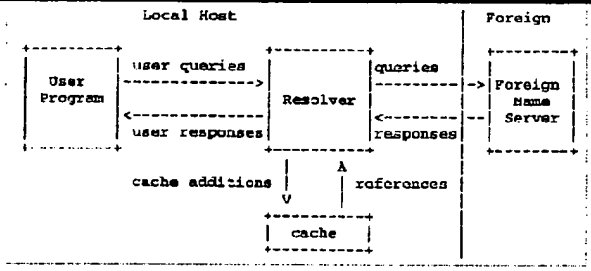
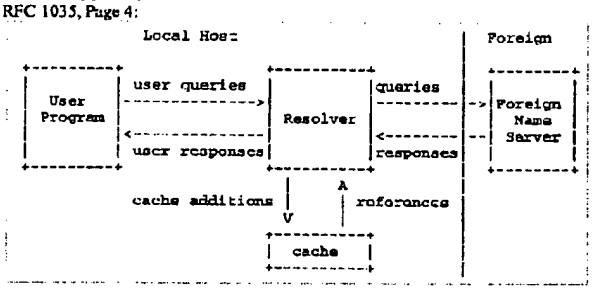
Petitioner Apple Inc. - Exhibit 1002, p. 646

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:	another network. VPNs accomplish this by allowing the user to *tunnel* through the Internet or another public network in a manner that provides the same security and features formerly available only in private networks (see Figure 1).  *Figure 1: Virtual Private Network* VPNs allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet). From the user's perspective, the VPN is a point-to-point connection between the user's computer and a corporate server. The nature of the intermediate internetwork is irrelevant to the user because it appears as if the data is being sent over a dedicated private link. VPN Overview, Page 9: By using a VPN, the network administrator can ensure that only those users on the corporate internetwork who have appropriate credentials (based on a need-to-know policy within the

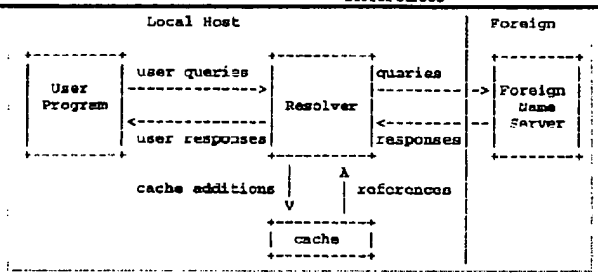
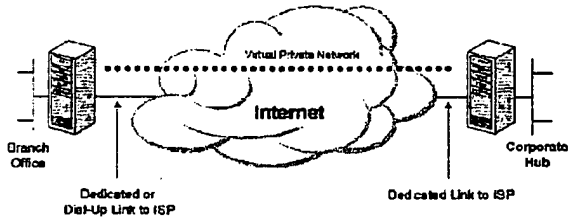
Petitioner Apple Inc. - Exhibit 1002, p. 647

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	company) can establish a VPN with the VPN server and gain access to the protected resources of the department. Additionally, all communication across the VPN can be encrypted for data confidentiality. Those users who do not have the proper credentials cannot view the department LAN. User Authentication. The solution must verify the user's identity and restrict VPN access to authorized users only. VPN Overview, Page 10:  *Figure 5: Tunneling* VPN Overview, Page 21: Voluntary tunneling occurs when a workstation or routing server uses tunneling client software to create a virtual connection to the target tunnel server.
receiving a secure domain name;	VPN Overview, Page 26: Redundancy and load balancing is accomplished using round-robin DNS to split requests among a number of VPN tunnel servers that share a common security perimeter. A security perimeter has one external DNS name--for example, vpnx.support.bigcompany.com--but several IP addresses, and loads are randomly distributed across all of the IP addresses. RFC 1035, Page 4:

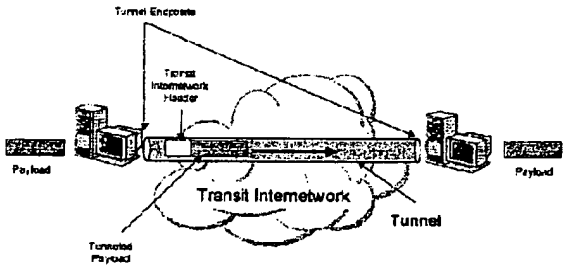
Petitioner Apple Inc. - Exhibit 1002, p. 648

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	
sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;	VPN Overview, Page 6: VPNs allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet). VPN Overview, Page 7: VPNs provide remote access to corporate resources over the public Internet, while maintaining privacy of information. RFC 1035, Page 4: 
receiving from the secure domain name service a response message containing the secure computer network	RFC 1035, Page 4:

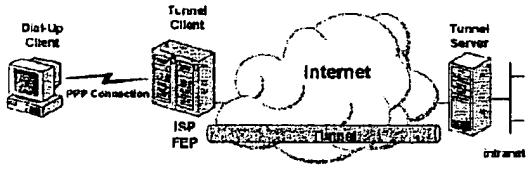
Petitioner Apple Inc. - Exhibit 1002, p. 649

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
address corresponding to the secure domain name; and	
sending an access request message to the secure computer network address using a virtual private network communication link.	VPN Overview, Page 6: VPNs allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet). VPN Overview, Page 7: VPNs provide remote access to corporate resources over the public Internet, while maintaining privacy of information. VPN Overview, Page 8: The VPN software uses the connection to the local ISP to create a virtual private network between the branch office router and the corporate hub router across the Internet.  *Figure 3: Using a VPN to connect two remote sites* VPN Overview, Page 9: By using a VPN, the network administrator can ensure that only those users on the corporate internetwork who have appropriate credentials (based on a need-to-know policy within the company) can establish a VPN with the VPN server and gain access to the protected resources of the

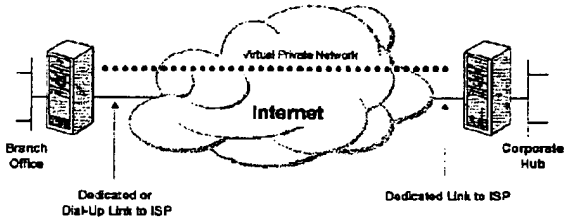
Petitioner Apple Inc. - Exhibit 1002, p. 650

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	department. Additionally, all communication across the VPN can be encrypted for data confidentiality. Those users who do not have the proper credentials cannot view the department LAN. User Authentication. The solution must verify the user's identity and restrict VPN access to authorized users only. VPN Overview, Page 10: Tunneling is a method of using an internetwork infrastructure to transfer data for one network over another network. The data to be transferred (or payload) can be the frames (or packets) of another protocol. Instead of sending a frame as it is produced by the originating node, the tunneling protocol encapsulates the frame in an additional header. The additional header provides routing information so that the encapsulated payload can traverse the intermediate internetwork. VPN Overview, Page 10:  *Figure 6: Tunneling* VPN Overview, Page 12: Once the tunnel is established, tunneled data can be sent. The tunnel client or server uses a tunnel data transfer protocol to prepare the data for transfer. For example, when the tunnel client sends a payload to the tunnel server, the tunnel client first appends a tunnel data transfer protocol header to the payload. The client then sends the resulting encapsulated payload across the internetwork, which routes it to the tunnel server. The tunnel server accepts the packets, removes the tunnel data transfer protocol header, and forwards the payload to the target network. Information sent between the tunnel server and the tunnel client behaves similarly. VPN Overview, Page 12: As a result, any user with access to one of the endpoint machines can use the tunnel. VPN Overview, Page 14: In the second phase, the client PC presents the user's credentials to the remote

Petitioner Apple Inc. - Exhibit 1002, p. 651

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	access server. A secure authentication scheme provides protection against replay attacks and remote client impersonation. VPN Overview, Page 22: This configuration is known as "compulsory" tunneling because the client is compelled to use the tunnel created by the FEP. Once the initial connection is made, all network traffic to and from the client is automatically sent through the tunnel. With compulsory tunneling, the client computer makes a single PPP connection, and when a client dials into the NAS, a tunnel is created and all traffic is automatically routed through the tunnel. VPN Overview, Page 22: In the Internet example, the client computer places a dial-up call to a tunneling-enabled NAS at the ISP. For example, a corporation may have contracted with and ISP to deploy a nationwide set of FEPs. These FEPs can establish tunnels across the Internet to a tunnel server connected to the corporation's private network, thereby consolidating calls from geographically diverse locations into a single Internet connection at the corporate network. VPN Overview, Page 22:  *Figure 9: Compulsory tunneling* VPN Overview, Pages 26-27: Redundancy and load balancing is accomplished using round-robin DNS to split requests among a number of VPN tunnel servers that share a common security perimeter. A security perimeter has one external DNS name—for example, vpnx.support.bigcompany.com—but several IP addresses, and loads are randomly distributed across all of the IP addresses. All of the servers can authenticate access requests against a shared database, such as a Windows NT Domain Controller. Note that Windows NT domain databases are replicated by design. VPN Overview, Page 28: As explained in this paper, VPNs allow users or corporations to connect to remote servers, branch offices, or to other companies over a public internetwork, while maintaining secure communications. In all of these cases, the secure connection across appears to the user as a private network communication-despite the fact that this communication occurs over a public internetwork.
35. The apparatus of claim 33, wherein	VPN Overview, Page 8: The VPN software uses the connection to the local ISP to create a virtual private

Petitioner Apple Inc. - Exhibit 1002, p. 652

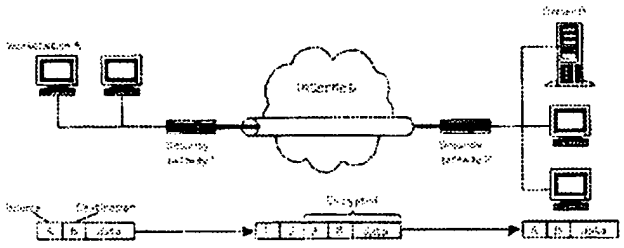
7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
the response message contains provisioning information for the virtual private network.	network between the branch office router and the corporate hub router across the Internet.  *Figure 3: Using a VPN to connect two remote sites* VPN Overview, Page 9: By using a VPN, the network administrator can ensure that only those users on the corporate internetwork who have appropriate credentials (based on a need-to-know policy within the company) can establish a VPN with the VPN server and gain access to the protected resources of the department. Additionally, all communication across the VPN can be encrypted for data confidentiality. Those users who do not have the proper credentials cannot view the department LAN. User Authentication. The solution must verify the user's identity and restrict VPN access to authorized users only. VPN Overview, Page 12: As a result, any user with access to one of the endpoint machines can use the tunnel. VPN Overview, Page 22: This configuration is known as "compulsory" tunneling because the client is compelled to use the tunnel created by the PEP. Once the initial connection is made, all network traffic to and from the client is automatically sent through the tunnel. With compulsory tunneling, the client computer makes a single PPP connection, and when a client dials into the NAS, a tunnel is created and all traffic is automatically routed through the tunnel. VPN Overview, Pages 26-27: Redundancy and load balancing is accomplished using round-robin DNS to split requests among a number of VPN tunnel servers that share a common security perimeter. A security perimeter has one external DNS name--for example, vpnx.support.bigcompany.com--but several IP addresses, and loads are randomly distributed across all of the IP addresses. All of the servers can authenticate access requests against a shared database, such as a Windows NT Domain Controller. Note that Windows NT domain databases are replicated by design. VPN Overview, Page 28: As explained in this paper, VPNs allow users or corporations to connect to remote servers, branch offices, or to other companies over a public internetwork, while maintaining secure communications. In all of these cases, the secure connection across appears to the user as a private network

Petitioner Apple Inc. - Exhibit 1002, p. 653

7,188,180 Claim Elements	Description for Claimed Elements in the VPN Overview and RFC 1035 Prior Art References
	communication-despite the fact that this communication occurs over a public internetwork.

Petitioner Apple Inc. - Exhibit 1002, p. 654

Appendix C
Citations to Exemplary Description in the Kosiur Reference*

7,188,180 Claim Elements	Deser for Claimed Elements in the Kosiur Prior Art Reference
1. A method for accessing a secure computer network address, comprising steps of:	Page 37: Internet VPN's go a step farther by offering businesses the opportunity to create these dynamic links over a variety of different transmission media, thus offering a single form of protected connectivity for both LANs at different sites and mobile workers. Page 40: Devices such as routers or switches that are part of the ISP's network are hidden from the devices and users of your virtual network. . . . Hiding the ISP and Internet infrastructure from your VPN applications is made possible by a concept called *tunneling*. Tunneling allows streams of data and associated user information to be transmitted over a shared network within a virtual *pipe*. This pipe makes the routed network totally transparent to users. Pages 41-42: Equally important to a VPN's use, if not more so, is the issue of privacy or security. In its more basic use, the "private" in VPN means that a tunnel between two users on a VPN appears as a private link, even if it's running over shared media. But, for business use, especially for LAN-to-LAN links, *private* has to mean more than that; it has to mean security, that is, freedom from prying eyes and tampering.  **FIGURE 3.2** Schematic of a tunnel. Page 379: Virtual Private Network (VPN) A private network built atop a public network (in this book, the Internet), in which secure connections are set up dynamically between a sender and a receiver.
receiving a secure domain name;	Page 36: If a corporate VPN is designed as one network with some special routed links called tunnels, full routing is possible between the parts of your network that are connected by tunnels, and you can use a single unified *Domain Name Service* (DNS) for resolving device names and IP addresses. This makes both reachability of hosts and routing more convenient and easier to manage. Page 293: The Domain Name Service (DNS) is the Internet's official naming system and is designed to name various network resources, including IP addresses. DNS is a distributed naming system--the database that translates names to objects is scattered across many thousands of host computers.

* - The cited passages are an indication of where in the Kosiur reference, at the very least, the claims find exemplary description. Requestor reserves the right to identify and demonstrate additional description if necessary or desirable.

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software. Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and you corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse. The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find. The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DSN server outside the firewall. If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.
sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;	Page 36: If a corporate VPN is designed as one network with some special routed links called tunnels, full routing is possible between the parts of your network that are connected by tunnels, and you can use a single unified *Domain Name Service* (DNS) for resolving device names and IP addresses. This makes both reachability of hosts and routing more convenient and easier to manage. Page 293: The Domain Name Service (DNS) is the Internet's official naming system and is designed to name various network resources, including IP addresses. DNS is a distributed naming system--the database that translates names to objects is scattered across many thousands of host computers. Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software. Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and you corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse.

Petitioner Apple Inc. - Exhibit 1002, p. 656

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find. The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DSN server outside the firewall. If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.
receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and	Page 293: Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software. Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and you corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse. The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find. The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DSN server outside the firewall. If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.
sending an access request message to the secure computer network address using a virtual private network communication link.	Page 40: In VPN's, "virtual" implies that the network is dynamic, with connections set up according to the organizational needs. Unlike the leased-line links used in traditional VPN's Internet VPN's do not maintain permanent links between the endpoints that make of the corporate network. Instead, a connection is created between two sites when it's needed. Pages 41-42: Equally important to a VPN's use, if not more so, is the issue of privacy or security. In its more basic use, the "private" in VPN means that a tunnel between two users on a VPN appears as a private link,

Petitioner Apple Inc. - Exhibit 1002, p. 657

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	even if it's running over shared media. But, for business use, especially for LAN-to-LAN links, *private* has to mean more than that; it has to mean security, that is, freedom from prying eyes and tampering.
4. The method according to claim 1, wherein the response message contains provisioning information for the virtual private network.	Page 40: In VPN's, "virtual" implies that the network is dynamic, with connections set up according to the organizational needs. Unlike the leased-line links used in traditional VPN's Internet VPN's do not maintain permanent links between the endpoints that make of the corporate network. Instead, a connection is created between two sites when it's needed. When the connection is no longer needed, it's torn down, making the bandwidth and other network resources available for other uses. Pages 41-42: Equally important to a VPN's use, if not more so, is the issue of privacy or security. In its more basic use, the "private" in VPN means that a tunnel between two users on a VPN appears as a private link, even if it's running over shared media. But, for business use, especially for LAN-to-LAN links, *private* has to mean more than that; it has to mean security, that is, freedom from prying eyes and tampering. Page 132: (4) Via RADIUS, the proxy server instructs the remote access server to grant (or deny) the user access. The remote access server will open the tunneled connection, creating a tunnel if necessary. Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and you corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse. The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find. The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DSN server outside the firewall. If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use. Pages 308 - 311: But, if traffic prioritization using classes is insufficient for your needs, and you choose to allocate network resources between real-time and non-real-time applications, then you have two choices. Either you can statically allocate the resources or you can allow resources to be reserved dynamically. *Static resource allocation* enables you to reserve a portion of a network's capacity for a particular type of traffic, usually based on protocol, application, or user. In many enterprise networks, routers are often

Petitioner Apple Inc. - Exhibit 1002, p. 658

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	configured to devote a certain amount of their capacity to SNA traffic, for instance, to accommodate the requirements of legacy data transactions. . . . . When the capacity is reserved for a specific protocol or application, the capacity should be large enough to meet the demands of all traffic of that type. If not, the traffic exceeding the allotted capacity will most likely be subject to delays and/or discards. If the allotted capacity isn't used, it's possible for other traffic to use the remaining bandwidth. . . . . RSVP operates on top of IP; it is an Internet control protocol like IGMP or ICMP, but it is not a routing protocol. It uses underlying routing protocols to determine the destination for reservation requests. As routing paths change, RSVP adapts its reservation to new paths if reservations are in place. The RSVP protocol is used by routers to deliver QoS control requests to all nodes along the paths of the flows (see Figure 15.3) and to establish and maintain state to provide the requested service. After a reservation has been made, routers supporting RSVP determine the route and the QoS class for each incoming packet and the scheduler makes forwarding decisions for every outgoing packet. Page 379: Virtual Private Network (VPN) A private network built atop a public network (in this book, the Internet), in which secure connections are set up dynamically between a sender and a receiver.
10. The method according to claim 1, wherein the virtual private network includes the Internet.	Page 37: Internet VPN's go a step farther by offering businesses the opportunity to create these dynamic links over a variety of different transmission media, thus offering a single form of protected connectivity for both LANs at different sites and mobile workers. Page 40: Devices such as routers or switches that are part of the ISP's network are hidden from the devices and users of your virtual network. . . . Hiding the ISP and Internet infrastructure from your VPN applications is made possible by a concept called *tunneling*. Page 379: Virtual Private Network (VPN) A private network built atop a public network (in this book, the Internet), in which secure connections are set up dynamically between a sender and a receiver.
12. The method of claim 1, wherein the access request message contains a request for information stored at the secure computer network address.	Page 40: Tunneling allows streams of data and associated user information to be transmitted over a shared network within a virtual *pipe*. This pipe makes the routed network totally transparent to users. Pages 41-42: Equally important to a VPN's use, if not more so, is the issue of privacy or security. In its more basic use, the "private" in VPN means that a tunnel between two users on a VPN appears as a private link, even if it's running over shared media. But, for business use, especially for LAN-to-LAN links, *private* has to mean more than that; it has to mean security, that is, freedom from prying eyes and tampering. Page 133: Upon authorization, the PPTP server will accept tunneled packets from the remote user and forward the packets to the appropriate destination on the corporate network. Pages 276 - 277: Before a secure tunnel can be established between two security gateways, or between a remote host and a gateway, these devices have to be authenticated by each other and agree on a key.

Petitioner Apple Inc. - Exhibit 1002, p. 659

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	. . . . If a security gateway isn't shipped with hard-wired keys, the gateway would be set to randomly generate its own key pair. A digital certificate then would be signed with the private key and sent to the appropriate certificate authority, either an in-house certificate server or a third-party CA like VeriSign. When the certificate is approved, that certificate is available from the CA for use by other security gateways and remote clients to authenticate the site before any data is exchanged (see Figure 13.2).
13. The method of claim 1,	
wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;	Page 36: If a corporate VPN is designed as one network with some special routed links called tunnels, full routing is possible between the parts of your network that are connected by tunnels, and you can use a single unified *Domain Name Service* (DNS) for resolving device names and IP addresses. This makes both reachability of hosts and routing more convenient and easier to manage. Page 293: The Domain Name Service (DNS) is the Internet's official naming system and is designed to name various network resources, including IP addresses. DNS is a distributed naming system—the database that translates names to objects is scattered across many thousands of host computers. Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software. Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and you corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse. The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find. The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DSN server outside the firewall. If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.

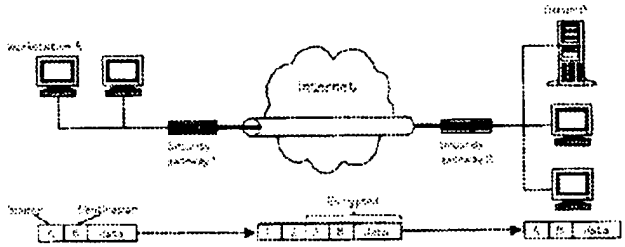
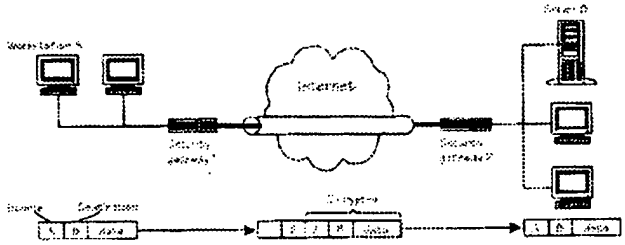
Petitioner Apple Inc. - Exhibit 1002, p. 660

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
wherein sending the query message comprises sending the query message at the client computer;	Page 36: If a corporate VPN is designed as one network with some special routed links called tunnels, full routing is possible between the parts of your network that are connected by tunnels, and you can use a single unified *Domain Name Service* (DNS) for resolving device names and IP addresses. This makes both reachability of hosts and routing more convenient and easier to manage. Page 293: The Domain Name Service (DNS) is the Internet's official naming system and is designed to name various network resources, including IP addresses. DNS is a distributed naming system--the database that translates names to objects is scattered across many thousands of host computers. Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software. Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and you corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse. The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find. The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DSN server outside the firewall. If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.
wherein receiving the response message comprises receiving the response message at the client computer,	Page 293: Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software. Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and you corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse.

Petitioner Apple Inc. - Exhibit 1002, p. 661

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find. The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DSN server outside the firewall. If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.
wherein sending the access request message comprises sending the access request message at the client computer.	Page 40: In VPN's, "virtual" implies that the network is dynamic, with connections set up according to the organizational needs. Unlike the leased-line links used in traditional VPN's Internet VPN's do not maintain permanent links between the endpoints that make of the corporate network. Instead, a connection is created between two sites when it's needed. Pages 41-42: Equally important to a VPN's use, if not more so, is the issue of privacy or security. In its more basic use, the "private" in VPN means that a tunnel between two users on a VPN appears as a private link, even if it's running over shared media. But, for business use, especially for LAN-to-LAN links, *private* has to mean more than that; it has to mean security, that is, freedom from prying eyes and tampering.
14. The method of claim 1, performed by a software module.	*See* claim 1, which is performed by software at the client computer (i.e., the VPN client). Page 37: Internet VPN's go a step farther by offering businesses the opportunity to create these dynamic links over a variety of different transmission media, thus offering a single form of protected connectivity for both LANs at different sites and mobile workers. Pages 41-42:

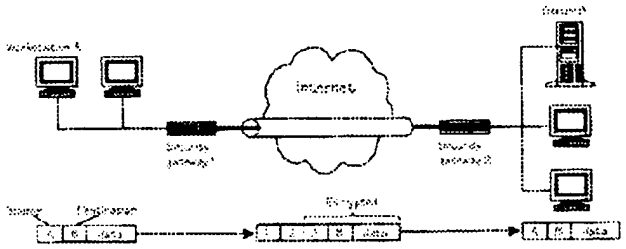
Petitioner Apple Inc. - Exhibit 1002, p. 662

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	 **FIGURE 3.2** Schematic of a tunnel. Page 161: If the ISP equipment supports L2TP, no additional software or hardware is required on the client end; only standard PPP software is necessary.
15. The method of claim 1, performed by a client computer.	*See* claim 1, which is performed by software at the client computer (i.e., the VPN client). Page 37: Internet VPN's go a step farther by offering businesses the opportunity to create these dynamic links over a variety of different transmission media, thus offering a single form of protected connectivity for both LANs at different sites and mobile workers. Pages 41-42:  **FIGURE 3.2** Schematic of a tunnel.

Petitioner Apple Inc. - Exhibit 1002, p. 663

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	Page 161: If the ISP equipment supports L2TP, no additional software or hardware is required on the client end; only standard PPP software is necessary. Page 379: Virtual Private Network (VPN) A private network built atop a public network (in this book, the Internet), in which secure connections are set up dynamically between a sender and a receiver.
17. A computer-readable storage medium, comprising:	Page 111: On the other hand, if you have mobile workers and small branch offices that will need to dial into the corporate net via an ISP, then IPSec client software has to be installed on the appropriate computers--laptops for the mobile workers, perhaps the branch office's desktop computers. Page 162: If you want end-to-end encryption, for instance, you would install IPSec-compliant clients on your mobile workers' computers and expect the ISP to handle encrypted packets from clients all the way to your network server.
a storage area; and	Page 111: On the other hand, if you have mobile workers and small branch offices that will need to dial into the corporate net via an ISP, then IPSec client software has to be installed on the appropriate computers--laptops for the mobile workers, perhaps the branch office's desktop computers. Page 162: If you want end-to-end encryption, for instance, you would install IPSec-compliant clients on your mobile workers' computers and expect the ISP to handle encrypted packets from clients all the way to your network server.
computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:	Page 37: Internet VPN's go a step farther by offering businesses the opportunity to create these dynamic links over a variety of different transmission media, thus offering a single form of protected connectivity for both LANs at different sites and mobile workers. Page 40: Devices such as routers or switches that are part of the ISP's network are hidden from the devices and users of your virtual network. . . . Hiding the ISP and Internet infrastructure from your VPN applications is made possible by a concept called *tunneling*. Tunneling allows streams of data and associated user information to be transmitted over a shared network within a virtual *pipe*. This pipe makes the routed network totally transparent to users. Pages 41-42: Equally important to a VPN's use, if not more so, is the issue of privacy or security. In its more basic use, the "private" in VPN means that a tunnel between two users on a VPN appears as a private link, even if it's running over shared media. But, for business use, especially for LAN-to-LAN links, *private* has to mean more than that; it has to mean security, that is, freedom from prying eyes and tampering.

Petitioner Apple Inc. - Exhibit 1002, p. 664

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	 **FIGURE 3.2** Schematic of a tunnel. Page 379: Virtual Private Network (VPN) A private network built atop a public network (in this book, the Internet), in which secure connections are set up dynamically between a sender and a receiver.
receiving a secure domain name;	Page 36: If a corporate VPN is designed as one network with some special routed links called tunnels, full routing is possible between the parts of your network that are connected by tunnels, and you can use a single unified *Domain Name Service* (DNS) for resolving device names and IP addresses. This makes both reachability of hosts and routing more convenient and easier to manage. Page 293: The Domain Name Service (DNS) is the Internet's official naming system and is designed to name various network resources, including IP addresses. DNS is a distributed naming system--the database that translates names to objects is scattered across many thousands of host computers. Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software. Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and you corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse. The solution is to install two corporate DNS servers, one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users

Petitioner Apple Inc. - Exhibit 1002, p. 665

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	will be able to find. The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DSN server outside the firewall. If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.
sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain name;	Page 36: If a corporate VPN is designed as one network with some special routed links called tunnels, full routing is possible between the parts of your network that are connected by tunnels, and you can use a single unified *Domain Name Service* (DNS) for resolving device names and IP addresses. This makes both reachability of hosts and routing more convenient and easier to manage. Page 293: The Domain Name Service (DNS) is the Internet's official naming system and is designed to name various network resources, including IP addresses. DNS is a distributed naming system—the database that translates names to objects is scattered across many thousands of host computers. Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software. Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and you corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse. The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find. The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DSN server outside the firewall. If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.
receiving from the domain name service a response message containing the secure computer network address corresponding to the secure domain name; and	Page 293: Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software.

Petitioner Apple Inc. - Exhibit 1002, p. 666

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and you corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse. The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find. The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DSN server outside the firewall. If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.
sending an access request message to the secure computer network address using a virtual private network communication link.	Page 40: In VPN's, "virtual" implies that the network is dynamic, with connections set up according to the organizational needs. Unlike the leased-line links used in traditional VPN's Internet VPN's do not maintain permanent links between the endpoints that make of the corporate network. Instead, a connection is created between two sites when it's needed. Pages 41 42: Equally important to a VPN's use, if not more so, is the issue of privacy or security. In its more basic use, the "private" in VPN means that a tunnel between two users on a VPN appears as a private link, even if it's running over shared media. But, for business use, especially for LAN-to-LAN links, *private* has to mean more than that; it has to mean security, that is, freedom from prying eyes and tampering.
20. The computer-readable medium according to claim 17, wherein the response message contains provisioning information for the virtual private network.	Page 40: In VPN's, "virtual" implies that the network is dynamic, with connections set up according to the organizational needs. Unlike the leased-line links used in traditional VPN's Internet VPN's do not maintain permanent links between the endpoints that make of the corporate network. Instead, a connection is created between two sites when it's needed. When the connection is no longer needed, it's torn down, making the bandwidth and other network resources available for other uses. Pages 41 42: Equally important to a VPN's use, if not more so, is the issue of privacy or security. In its more basic use, the "private" in VPN means that a tunnel between two users on a VPN appears as a private link, even if it's running over shared media. But, for business use, especially for LAN to LAN links, *private* has to mean more than that; it has to mean security, that is, freedom from prying eyes and tampering. Page 132: (4) Via RADIUS, the proxy server instructs the remote access server to grant (or deny) the user access. The remote access server will open the tunneled connection, creating a tunnel if necessary.

Petitioner Apple Inc. - Exhibit 1002, p. 667

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and you corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse. The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find. The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DSN server outside the firewall. If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use. Pages 308 - 311: But, if traffic prioritization using classes is insufficient for your needs, and you choose to allocate network resources between real-time and non-real-time applications, then you have two choices. Either you can statically allocate the resources or you can allow resources to be reserved dynamically. *Static resource allocation* enables you to reserve a portion of a network's capacity for a particular type of traffic, usually based on protocol, application, or user. In many enterprise networks, routers are often configured to devote a certain amount of their capacity to SNA traffic, for instance, to accommodate the requirements of legacy data transactions. . . . . When the capacity is reserved for a specific protocol or application, the capacity should be large enough to meet the demands of all traffic of that type. If not, the traffic exceeding the allotted capacity will most likely be subject to delays and/or discards. If the allotted capacity isn't used, it's possible for other traffic to use the remaining bandwidth. . . . . RSVP operates on top of IP; it is an Internet control protocol like IGMP or ICMP, but it is not a routing protocol. It uses underlying routing protocols to determine the destination for reservation requests. As routing paths change, RSVP adapts its reservation to new paths if reservations are in place. The RSVP protocol is used by routers to deliver QoS control requests to all nodes along the paths of the flows (see Figure 15.3) and to establish and maintain state to provide the requested service. After a reservation has been made, routers supporting RSVP determine the route and the QoS class for each incoming packet and the scheduler makes forwarding decisions for every outgoing packet.

Petitioner Apple Inc. - Exhibit 1002, p. 668

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	Page 379: Virtual Private Network (VPN) A private network built atop a public network (in this book, the Internet), in which secure connections are set up dynamically between a sender and a receiver.
26. The computer-readable medium according to claim 17, wherein the virtual private network includes the Internet.	Page 37: Internet VPN's go a step farther by offering businesses the opportunity to create these dynamic links over a variety of different transmission media, thus offering a single form of protected connectivity for both LANs at different sites and mobile workers. Page 40: Devices such as routers or switches that are part of the ISP's network are hidden from the devices and users of your virtual network. . . . Hiding the ISP and Internet infrastructure from your VPN applications is made possible by a concept called *tunneling*. Page 379: Virtual Private Network (VPN) A private network built atop a public network (in this book, the Internet), in which secure connections are set up dynamically between a sender and a receiver.
28. The computer readable medium of claim 17, wherein the access request message contains a request for information stored at the secure computer network address.	Page 40: Tunneling allows streams of data and associated user information to be transmitted over a shared network within a virtual *pipe*. This pipe makes the routed network totally transparent to users. Pages 41-42: Equally important to a VPN's use, if not more so, is the issue of privacy or security. In its more basic use, the "private" in VPN means that a tunnel between two users on a VPN appears as a private link, even if it's running over shared media. But, for business use, especially for LAN-to-LAN links, *private* has to mean more than that; it has to mean security, that is, freedom from prying eyes and tampering. Page 133: Upon authorization, the PPTP server will accept tunneled packets from the remote user and forward the packets to the appropriate destination on the corporate network. Pages 276 - 277: Before a secure tunnel can be established between two security gateways, or between a remote host and a gateway, these devices have to be authenticated by each other and agree on a key. . . . . If a security gateway isn't shipped with hard-wired keys, the gateway would be set to randomly generate its own key pair. A digital certificate then would be signed with the private key and sent to the appropriate certificate authority, either an in-house certificate server or a third-party CA like VeriSign. When the certificate is approved, that certificate is available from the CA for use by other security gateways and remote clients to authenticate the site before any data is exchanged (see Figure 13.2).
29. The computer-readable medium according to claim 17,	
wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;	Page 36: If a corporate VPN is designed as one network with some special routed links called tunnels, full routing is possible between the parts of your network that are connected by tunnels, and you can use a single unified *Domain Name Service* (DNS) for resolving device names and IP addresses. This makes both

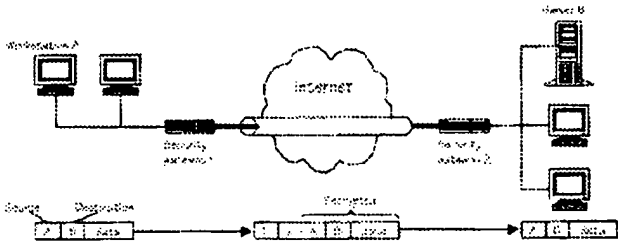
Petitioner Apple Inc. - Exhibit 1002, p. 669

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	reachability of hosts and routing more convenient and easier to manage. Page 293: The Domain Name Service (DNS) is the Internet's official naming system and is designed to name various network resources, including IP addresses. DNS is a distributed naming system--the database that translates names to objects is scattered across many thousands of host computers. Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software. Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and you corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse. The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find. The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DSN server outside the firewall. If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.
wherein sending the query message comprises sending the query message at the client computer;	Page 36: If a corporate VPN is designed as one network with some special routed links called tunnels, full routing is possible between the parts of your network that are connected by tunnels, and you can use a single unified *Domain Name Service* (DNS) for resolving device names and IP addresses. This makes both reachability of hosts and routing more convenient and easier to manage. Page 293: The Domain Name Service (DNS) is the Internet's official naming system and is designed to name various network resources, including IP addresses. DNS is a distributed naming system--the database that translates names to objects is scattered across many thousands of host computers. Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software. Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access

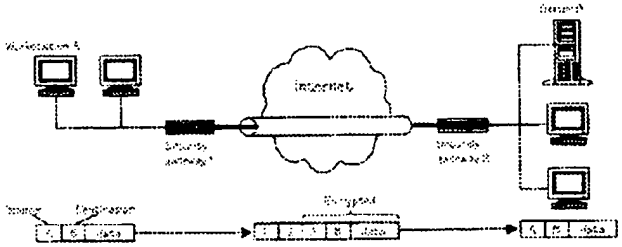
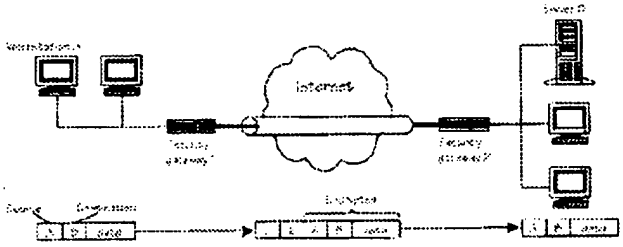
Petitioner Apple Inc. - Exhibit 1002, p. 670

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and you corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse. The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find. The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DSN server outside the firewall. If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.
wherein receiving the response message comprises receiving the response message at the client computer,	Page 293: Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software. Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and you corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse. The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find. The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DSN server outside the firewall. If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.
wherein sending the access request message comprises sending the access request	Page 40: In VPN's, "virtual" implies that the network is dynamic, with connections set up according to the organizational needs. Unlike the leased-line links used in traditional VPN's Internet VPN's do not maintain

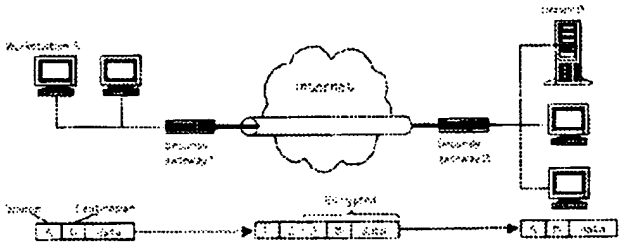
Petitioner Apple Inc. - Exhibit 1002, p. 671

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
message at the client computer.	permanent links between the endpoints that make of the corporate network. Instead, a connection is created between two sites when it's needed. Pages 41-42: Equally important to a VPN's use, if not more so, is the issue of privacy or security. In its more basic use, the "private" in VPN means that a tunnel between two users on a VPN appears as a private link, even if it's running over shared media. But, for business use, especially for LAN-to-LAN links, *private* has to mean more than that; it has to mean security, that is, freedom from prying eyes and tampering.
30. The computer-readable medium according to claim 17, wherein the method is performed by a software module.	*See* claim 1, which is performed by software at the client computer (i.e., the VPN client). Page 37: Internet VPN's go a step farther by offering businesses the opportunity to create these dynamic links over a variety of different transmission media, thus offering a single form of protected connectivity for both LANs at different sites and mobile workers. Pages 41-42:  **FIGURE 3.2** Schematic of a tunnel. Page 161: If the ISP equipment supports L2TP, no additional software or hardware is required on the client end; only standard PPP software is necessary.
31. The computer-readable medium according to claim 17, wherein the method is performed by a client computer.	*See* claim 1, which is performed by software at the client computer (i.e., the VPN client). Page 37: Internet VPN's go a step farther by offering businesses the opportunity to create these dynamic links over a variety of different transmission media, thus offering a single form of protected connectivity for both LANs at different sites and mobile workers. Pages 41-42:

Petitioner Apple Inc. - Exhibit 1002, p. 672

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	 FIGURE 3.2 Schematic of a tunnel. Page 161: If the ISP equipment supports L2TP, no additional software or hardware is required on the client end; only standard PPP software is necessary. Page 379: Virtual Private Network (VPN) A private network built atop a public network (in this book, the Internet), in which secure connections are set up dynamically between a sender and a receiver.
33. A data processing apparatus, comprising:	Page 41:  FIGURE 3.2 Schematic of a tunnel.
a processor, and	Page 34: Another factor of great importance to network managers is the reliability of the product or service. For VPNs, reliability concerns focus on two different components-the hardware (and associated software)

Petitioner Apple Inc. - Exhibit 1002, p. 673

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	and the communications services (i.e., the Internet). Using standard components in the hardware-microprocessors, proven interface cards, and so on-is important, as is the maintainability of the hardware.
memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:	Page 37: Internet VPN's go a step farther by offering businesses the opportunity to create these dynamic links over a variety of different transmission media, thus offering a single form of protected connectivity for both LANs at different sites and mobile workers. Page 40: Devices such as routers or switches that are part of the ISP's network are hidden from the devices and users of your virtual network. . . . Hiding the ISP and Internet infrastructure from your VPN applications is made possible by a concept called *tunneling*. Tunneling allows streams of data and associated user information to be transmitted over a shared network within a virtual *pipe*. This pipe makes the routed network totally transparent to users. Pages 41-42: Equally important to a VPN's use, if not more so, is the issue of privacy or security. In its more basic use, the "private" in VPN means that a tunnel between two users on a VPN appears as a private link, even if it's running over shared media. But, for business use, especially for LAN-to-LAN links, *private* has to mean more than that; it has to mean security, that is, freedom from prying eyes and tampering.  **FIGURE 3.2** Schematic of a tunnel. Page 379: Virtual Private Network (VPN) A private network built atop a public network (in this book, the Internet), in which secure connections are set up dynamically between a sender and a receiver.
receiving a secure domain name;	Page 36: If a corporate VPN is designed as one network with some special routed links called tunnels, full routing is possible between the parts of your network that are connected by tunnels, and you can use a single unified *Domain Name Service* (DNS) for resolving device names and IP addresses. This makes both reachability of hosts and routing more convenient and easier to manage. Page 293: The Domain Name Service (DNS) is the Internet's official naming system and is designed to name various network resources, including IP addresses. DNS is a distributed naming system—the database that translates names to objects is scattered across many thousands of host computers.

Petitioner Apple Inc. - Exhibit 1002, p. 674

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software. Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and you corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse. The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find. The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DSN server outside the firewall. If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.
sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;	Page 36: If a corporate VPN is designed as one network with some special routed links called tunnels, full routing is possible between the parts of your network that are connected by tunnels, and you can use a single unified *Domain Name Service* (DNS) for resolving device names and IP addresses. This makes both reachability of hosts and routing more convenient and easier to manage. Page 293: The Domain Name Service (DNS) is the Internet's official naming system and is designed to name various network resources, including IP addresses. DNS is a distributed naming system--the database that translates names to objects is scattered across many thousands of host computers. Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software. Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and you corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse.

Petitioner Apple Inc. - Exhibit 1002, p. 675

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find. The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DSN server outside the firewall. If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.
receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and	Page 293: Domain name requests (i.e., requests to convert a network name into its corresponding network address) are handled by a hierarchy of DNS servers (see Figure 14.2). Requests are sent first to the local (i.e., lowest level) nameserver in the network hierarchy, with the IP address of this nameserver typically configured in each workstation's TCP/IP software. Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and you corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse. The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find. The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DSN server outside the firewall. If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use.
sending an access request message to the secure computer network address using a virtual private network communication link.	Page 40: In VPN's, "virtual" implies that the network is dynamic, with connections set up according to the organizational needs. Unlike the leased-line links used in traditional VPN's Internet VPN's do not maintain permanent links between the endpoints that make of the corporate network. Instead, a connection is created between two sites when it's needed. Pages 41-42: Equally important to a VPN's use, if not more so, is the issue of privacy or security. In its more basic use, the "private" in VPN means that a tunnel between two users on a VPN appears as a private link,

Petitioner Apple Inc. - Exhibit 1002, p. 676

7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	even if it's running over shared media. But, for business use, especially for LAN-to-LAN links, *private* has to mean more than that; it has to mean security, that is, freedom from prying eyes and tampering.
35. The apparatus of claim 33, wherein the response message contains provisioning information for the virtual private network.	Page 40: In VPN's, "virtual" implies that the network is dynamic, with connections set up according to the organizational needs. Unlike the leased-line links used in traditional VPN's Internet VPN's do not maintain permanent links between the endpoints that make of the corporate network. Instead, a connection is created between two sites when it's needed. When the connection is no longer needed, it's torn down, making the bandwidth and other network resources available for other uses. Pages 41-42: Equally important to a VPN's use, if not more so, is the issue of privacy or security. In its more basic use, the "private" in VPN means that a tunnel between two users on a VPN appears as a private link, even if it's running over shared media. But, for business use, especially for LAN-to-LAN links, *private* has to mean more than that; it has to mean security, that is, freedom from prying eyes and tampering. Page 132: (4) Via RADIUS, the proxy server instructs the remote access server to grant (or deny) the user access. The remote access server will open the tunneled connection, creating a tunnel if necessary. Page 296: To properly map names to addresses, your corporate DNS server has to communicate with an external DNS server, presumably one hosted by your ISP. But, because you don't want outsiders to access your internal resources, you need to protect your internal DNS server (along with other network resources), so you install a firewall. Since the ISP's DNS server is outside the firewall, and you corporate DNS server is inside the firewall, they cannot readily communicate, which keeps employees from accessing outside resources as well as the reverse. The solution is to install two corporate DNS servers: one on the outside of the firewall and one inside it. This is the double DNS scheme. The next step is to separate the hosts that had been on your sole DNS server into two groups. The first group lists those hosts that you want anyone on the Internet to find, such as your e-mail gateway, public Web site, and anonymous FTP server, for instance; it'll also include the name of the firewall's external interface. The second list contains the set of hosts that only your internal network users will be able to find. The hosts on your internal network use the internal DNS server as their primary DNS server. When they want to access external hosts, the internal DNS server will forward DNS resolution request to the external DSN server outside the firewall. If you intend to allow access to a limited number of hosts on your VPN, then you could try maintaining dual DNS entries: one set for internal usage and the second for VPN use. Pages 308 - 311: But, if traffic prioritization using classes is insufficient for your needs, and you choose to allocate network resources between real-time and non-real-time applications, then you have two choices. Either you can statically allocate the resources or you can allow resources to be reserved dynamically. *Static resource allocation* enables you to reserve a portion of a network's capacity for a particular type of traffic, usually based on protocol, application, or user. In many enterprise networks, routers are often

Petitioner Apple Inc. - Exhibit 1002, p. 677

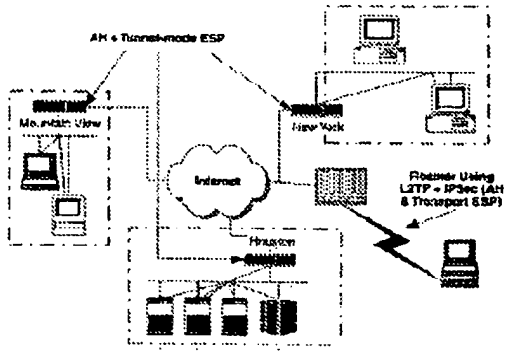
7,188,180 Claim Elements	Descr for Claimed Elements in the Kosiur Prior Art Reference
	configured to devote a certain amount of their capacity to SNA traffic, for instance, to accommodate the requirements of legacy data transactions. . . . . When the capacity is reserved for a specific protocol or application, the capacity should be large enough to meet the demands of all traffic of that type. If not, the traffic exceeding the allotted capacity will most likely be subject to delays and/or discards. If the allotted capacity isn't used, it's possible for other traffic to use the remaining bandwidth. . . . . RSVP operates on top of IP; it is an Internet control protocol like IGMP or ICMP, but it is not a routing protocol. It uses underlying routing protocols to determine the destination for reservation requests. As routing paths change, RSVP adapts its reservation to new paths if reservations are in place. The RSVP protocol is used by routers to deliver QoS control requests to all nodes along the paths of the flows (see Figure 15.3) and to establish and maintain state to provide the requested service. After a reservation has been made, routers supporting RSVP determine the route and the QoS class for each incoming packet and the scheduler makes forwarding decisions for every outgoing packet. Page 379: Virtual Private Network (VPN) A private network built atop a public network (in this book, the Internet), in which secure connections are set up dynamically between a sender and a receiver.

Petitioner Apple Inc. - Exhibit 1002, p. 678

Appendix D
Citations to Exemplary Description in the Kaufman Reference*

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
1. A method for accessing a secure computer network address, comprising steps of:	Page 2: The IPsec protocols were designed to clear the hit list of well-known security flaws in the current Internet Protocol version 4 (IPv4) and to provide a preemptive strike against these same flaws in its possible replacement, the Internet Protocol version 6 (IPv6). They provide standard, highly generalized, cryptographic security mechanisms for authentication, access control, confidentiality, data integrity, replay protection, and protection against traffic flow analysis. Page 9: As Dynamic Host Configuration Protocol (DHCP) becomes prevalent and people need access to data from more locations inside and outside your company, your security solutions will need to adapt to a dynamic IP network in order to authenticate users and enforce security principles. In the past, both users and IP addresses tended to be static. The average person might have had one address for his PC or workstation on the corporate LAN and another for his home SLIP or PPP connection. Today corporate users often drag their laptops around with them and obtain new addresses every time they restart their machines. They expect to work on business trips from airports, from hotels, or even from networks at other companies. Security perimeters can no longer work from static rules that associate a person with one or two IP addresses. Instead, they must rely on various user authentication technologies to identify users and their privileges, while also taking into account any additional constraints associated with a given user's current physical location. Page 140: Businesses generally deploy IPsec gateway-to-gateway (or network-to-network) as a secure alternative to a private WAN or leased-line connection. . . . . An extranet is an instance of a virtual private network (VPN), described in the section that follows. Because an extranet involves a trust relationship among entities that are not part of a single trust hierarchy, either each gateway needs to participate in each organization's PKI or each organization needs to deploy a PKI capable of cross-certifying portions of its trust hierarchy. Pages 141-142: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs. End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider. A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.

* - The cited passages are an indication of where in the Kaufman reference, at the very least, the claims find exemplary description. Requestor reserves the right to identify and demonstrate additional description if necessary or desirable.

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	 Figure 9.1 IPsec VPN Page 200: The simplest form of management is manual management, in which a person manually configures each system with keying material and security association management data relevant to secure communication with other systems. Manual techniques are practical in small, static environments but they do not scale well. For example, a company could create a Virtual Private Network (VPN) using IPsec in security gateways at several sites. If the number of sites is small, and since all the sites come under the purview of a single administrative domain, this is likely to be a feasible context for manual management techniques. In this case, the security gateway might selectively protect traffic to and from other sites within the organization using a manually configured key, while not protecting traffic for other destinations.
receiving a secure domain name;	Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel. Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of *name-to-address* and *address-to-name* mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or *resolve)* a name to an address (or vice versa) and a server-to-server update mechanism called a *zone transfer.*

Petitioner Apple Inc. - Exhibit 1002, p. 680

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF *DNS Security* (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137). Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the *secure* IP address) in one that is routable from the given location. Page 191: 1. User ID a. a fully qualified user name string (DNS). e.g., mozart@foo.bar.com Page 243: *Domain Name Service*. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.
sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;	Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel. Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of *name-to-address* and *address-to-name* mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or *resolve*) a name to an address (or vice versa) and a server-to-server update mechanism called a *zone transfer*. Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF *DNS Security* (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137). Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the *secure* IP address) in one that is routable from the given location.

Petitioner Apple Inc. - Exhibit 1002, p. 681

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	Page 191: 1. User ID a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com Page 243: *Domain Name Service.* The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.
receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and	Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel. Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of *name-to-address* and *address-to-name* mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or *resolve)* a name to an address (or vice versa) and a server-to-server update mechanism called a *zone transfer.* Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF *DNS Security* (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137) Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the *secure* IP address) in one that is routable from the given location. Page 191: 1. User ID a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com Page 243: *Domain Name Service.* The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.
sending an access request message to the secure computer network address using a virtual private network communication link.	Page 65: People and businesses who use IP networks tend to do so with the assumption that they can trust the origin and content of the data they work with, and that their transactions, if not secret, are reasonably private. Page 94: In theory, devices or services that authenticate using certificates must retrieve a current CRL before enabling access or establishing communication. Page 141: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs.

Petitioner Apple Inc. - Exhibit 1002, p. 682

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider. Page 142: A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.
4. The method according to claim 1, wherein the response message contains provisioning information for the virtual private network.	Page 121: RSVP is a signaling protocol used to negotiate in advance a hop-by-hop bandwidth reservation for specified traffic (Braden 1997). It does not carry data, but rather negotiates on behalf of an application. To request bandwidth, an RSVP-enabled application sends a PATH request toward its destination, including a traffic specification for the application and a request for some amount of bandwidth allocation. RSVP capable gateways reply back with RESV reservation responses. Application traffic then follows the signaling path across the network. RSVP arranges for only a unidirectional bandwidth allocation. It is designed to support applications that need significant available one-way bandwidth, such as streaming audio or video. If an application has significant bi- or multidirectional traffic requirements, each traffic originator must negotiate separately for bandwidth reservations.
10. The method according to claim 1, wherein the virtual private network includes the Internet.	Page 12: While you probably already know how the major parts of your network hang together, you probably do not have a comparable grasp of all the external connections that terminate somewhere inside your network perimeter. These connections may include lines leased to other organizations, departmental remote access servers and Internet connections, and analog or digital dial-up devices on individual networkconnected PCs. Pages 100-101: The standardization of a general-purpose secure transmission mechanism for IP has several advantages. It is very consistent with the overall layered design of the Internet, where protocols are intended to integrate without overt reference to or dependencies on one another. Page 126: Unfortunately, the places where IPsec might offer the most benefit are also the places where it is most difficult to deploy-in the core of the Internet and at peering points among multiple service providers. The challenge at administrative boundaries is not IPsec, but trust. Correct authentication of the IPsec peers requires either shared secrets-which are difficult to administer and almost impossible to scale--or some form of cross-certification among PKIs, which essentially requires (today) that all PKIs come from a single vendor.
12. The method of claim 1, wherein the access request message contains a request for information stored at the secure computer network address.	Page 65: People and businesses who use IP networks tend to do so with the assumption that they can trust the origin and content of the data they work with, and that their transactions, if not secret, are reasonably private. Page 94: In theory, devices or services that authenticate using certificates must retrieve a current CRL before enabling access or establishing communication. Page 141: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as

Petitioner Apple Inc. - Exhibit 1002, p. 683

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs. End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider. Page 142: A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.
13. The method of claim 1,	
wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;	Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel. Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of *name-to-address* and *address-to-name* mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or *resolve)* a name to an address (or vice versa) and a server-to-server update mechanism called a *zone transfer.* Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF *DNS Security* (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137). Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the *secure* IP address) in one that is routable from the given location. Page 191: 1. User ID a. a fully qualified user name string (DNS), e.g., mozart@foo.bar.com Page 243: *Domain Name Service.* The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.
wherein sending the query message comprises sending the query message at the	Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as

Petitioner Apple Inc. - Exhibit 1002, p. 684

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
client computer;	dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel. Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of *name-to-address* and *address-to-name* mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or *resolve)* a name to an address (or vice versa) and a server-to-server update mechanism called a *zone transfer.* Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF *DNS Security* (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137) Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the *secure* IP address) in one that is routable from the given location. Page 191: 1. User ID a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com Page 243: *Domain Name Service.* The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.
wherein receiving the response message comprises receiving the response message at the client computer,	Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel. Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of *name-to-address* and *address-to-name* mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or *resolve)* a name to an address (or vice versa) and a server-to-server update mechanism called a *zone transfer.* Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF *DNS Security* (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see

Petitioner Apple Inc. - Exhibit 1002, p. 685

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	RFC 2065 and RFC 2137). Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the *secure* IP address) in one that is routable from the given location. Page 191: 1. User ID a. a fully qualified user name string (DNS), e.g., mozart@foo.bar.com Page 243: *Domain Name Service*. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.
wherein sending the access request message comprises sending the access request message at the client computer.	Page 65: People and businesses who use IP networks tend to do so with the assumption that they can trust the origin and content of the data they work with, and that their transactions, if not secret, are reasonably private. Page 94: In theory, devices or services that authenticate using certificates must retrieve a current CRL before enabling access or establishing communication. Page 141: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs. End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider. Page 142: A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.
14. The method of claim 1, performed by a software module.	Page 133: Many network devices use *Trivial File Transfer Protocol* (TFTP) to retrieve new versions of software from a TFTP server (usually a UNIX host) and to upload copies of their running configurations, core dumps, error messages, or other diagnostics. Page 180: Integration of IPsec into the native IP implementation. This requires access to the IP source code and is applicable to both hosts and security gateways. Page 222: IPsec always has to figure out what the encapsulating IP header fields are. This is independent of where you insert IPsec and is intrinsic to the definition of IPsec. Therefore any IPsec implementation that is not integrated into an IP implementation must include code to construct the necessary IP headers (e.g., IP2):
15. The method of claim 1, performed by a client computer.	Pages 141-142: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as

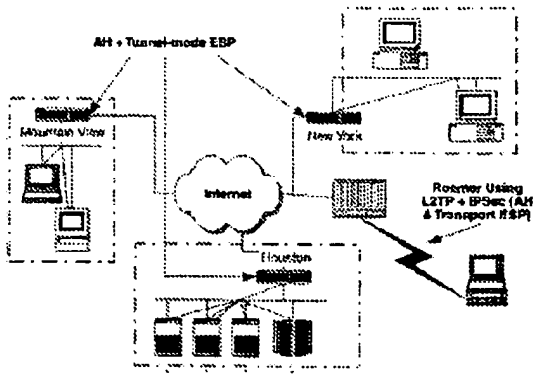
Petitioner Apple Inc. - Exhibit 1002, p. 686

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs. End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider. A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network. Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the *secure* IP address) in one that is routable from the given location.
17. A computer-readable storage medium, comprising:	Page 215: The use of IPsec imposes computational performance costs on the hosts or security gateways that implement these protocols. These costs are associated with the memory needed for IPsec code and data structures, and the computation of integrity check values, encryption and decryption, and added per-packet handling. The per-packet computational costs will be manifested by increased latency and, possibly, reduced throughput. Use of SA/key management protocols, especially ones that employ public key cryptography, also adds computational performance costs to use of IPsec. These per association computational costs will be manifested in terms of increased latency in association establishment. For many hosts, it is anticipated that software-based cryptography will not appreciably reduce throughput, but hardware may be required for security gateways (since they represent aggregation points), and for some hosts.
a storage area; and	Page 215: The use of IPsec imposes computational performance costs on the hosts or security gateways that implement these protocols. These costs are associated with the memory needed for IPsec code and data structures, and the computation of integrity check values, encryption and decryption, and added per-packet handling.
computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:	Page 2: The IPsec protocols were designed to clear the hit list of well-known security flaws in the current Internet Protocol version 4 (IPv4) and to provide a preemptive strike against these same flaws in its possible replacement, the Internet Protocol version 6 (IPv6). They provide standard, highly generalized, cryptographic security mechanisms for: authentication, access control, confidentiality, data integrity, replay protection, and protection against traffic flow analysis. Page 9: As Dynamic Host Configuration Protocol (DHCP) becomes prevalent and people need access to data from more locations inside and outside your company, your security solutions will need to adapt to a dynamic IP network in order to authenticate users and enforce security principles. In the past, both users and

Petitioner Apple Inc. - Exhibit 1002, p. 687

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	IP addresses tended to be static. The average person might have had one address for his PC or workstation on the corporate LAN and another for his home SLIP or PPP connection. Today corporate users often drag their laptops around with them and obtain new addresses every time they restart their machines. They expect to work on business trips from airports, from hotels, or even from networks at other companies. Security perimeters can no longer work from static rules that associate a person with one or two IP addresses. Instead, they must rely on various user authentication technologies to identify users and their privileges, while also taking into account any additional constraints associated with a given user's current physical location. Page 83: Insert the ESP header, payload, and trailer (plus authentication/integrity data) directly after the IP header. (Note that in IPv6, the ESP data belongs after all of the hop-by-hop headers.) Pages 103-104: Most current commercial IPsec products are software implementations on a general-purpose CPU with some hardware components to accelerate cryptographic operations. Software products have the advantage of being relatively easy to modify, but they can encounter memory constraints, processor restrictions, and arbitrary-seeming configuration limitations. Page 129: Host-based systems are software packages that scan traffic coming in to a particular end host. Intrusion detection is one of the few real-time security technologies that can be configured to adapt to the actual operating characteristics of a network and can also provide rapid, specific countermeasures in the event of a possible attack. Page 140: Businesses generally deploy IPsec gateway-to-gateway (or network-to-network) as a secure alternative to a private WAN or leased-line connection. . . . . An extranet is an instance of a *virtual private network* (VPN), described in the section that follows. Because an extranet involves a trust relationship among entities that are not part of a single trust hierarchy, either each gateway needs to participate in each organization's PKI or each organization needs to deploy a PKI capable of cross-certifying portions of its trust hierarchy. Pages 141-142: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs. End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider. A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.

Petitioner Apple Inc. - Exhibit 1002, p. 688

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	 Figure 9.1 IPsec VPN.
receiving a secure domain name;	Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel. Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of *name-to-address* and *address-to-name* mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or *resolve)* a name to an address (or vice versa) and a server-to-server update mechanism called a *zone transfer.* Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF *DNS Security* (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137)

Petitioner Apple Inc. - Exhibit 1002, p. 689

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the *secure* IP address) in one that is routable from the given location. Page 191: 1. User ID a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com Page 243: *Domain Name Service*. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.
sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain name;	Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel. Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of *name-to-address* and *address-to-name* mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or *resolve*) a name to an address (or vice versa) and a server-to-server update mechanism called a *zone transfer*. Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF *DNS Security* (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137). Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the *secure* IP address) in one that is routable from the given location. Page 191: 1. User ID a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com Page 243: *Domain Name Service*. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.
receiving from the domain	Page 125: The technologies described in the following sections are among those vital to network operation.

Petitioner Apple Inc. - Exhibit 1002, p. 690

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
name service a response message containing the secure computer network address corresponding to the secure domain name; and	If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel. Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of *name-to-address* and *address-to-name* mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or *resolve)* a name to an address (or vice versa) and a server-to-server update mechanism called a *zone transfer.* Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF *DNS Security* (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137). Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the *secure* IP address) in one that is routable from the given location. Page 191: 1. User ID a. a fully qualified user name string (DNS), e.g., mozart@foo.bar.com Page 243: *Domain Name Service.* The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.
sending an access request message to the secure computer network address using a virtual private network communication link.	Page 65: People and businesses who use IP networks tend to do so with the assumption that they can trust the origin and content of the data they work with, and that their transactions, if not secret, are reasonably private. Page 94: In theory, devices or services that authenticate using certificates must retrieve a current CRL before enabling access or establishing communication. Page 141: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs. End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider. Page 142: A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote

Petitioner Apple Inc. - Exhibit 1002, p. 691

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	host can receive an IP address internal to its home network.
20. The computer-readable medium according to claim 17, wherein the response message contains provisioning information for the virtual private network.	Page 121: RSVP is a signaling protocol used to negotiate in advance a hop-by-hop bandwidth reservation for specified traffic (Braden 1997). It does not carry data, but rather negotiates on behalf of an application. To request bandwidth, an RSVP-enabled application sends a PATH request toward its destination, including a traffic specification for the application and a request for some amount of bandwidth allocation. RSVP capable gateways reply back with RESV reservation responses. Application traffic then follows the signaling path across the network. RSVP arranges for only a unidirectional bandwidth allocation. It is designed to support applications that need significant available one-way bandwidth, such as streaming audio or video. If an application has significant bi- or multidirectional traffic requirements, each traffic originator must negotiate separately for bandwidth reservations.
26. The computer-readable medium according to claim 17, wherein the virtual private network includes the Internet.	Page 12: While you probably already know how the major parts of your network hang together, you probably do not have a comparable grasp of all the external connections that terminate somewhere inside your network perimeter. These connections may include lines leased to other organizations, departmental remote access servers and Internet connections, and analog or digital dial-up devices on individual networkconnected PCs. Pages 100-101: The standardization of a general-purpose secure transmission mechanism for IP has several advantages. It is very consistent with the overall layered design of the Internet, where protocols are intended to integrate without overt reference to or dependencies on one another. Page 126: Unfortunately, the places where IPsec might offer the most benefit are also the places where it is most difficult to deploy-in the core of the Internet and at peering points among multiple service providers. The challenge at administrative boundaries is not IPsec, but trust. Correct authentication of the IPsec peers requires either shared secrets-which are difficult to administer and almost impossible to scale--or some form of cross-certification among PKIs, which essentially requires (today) that all PKIs come from a single vendor.
28. The computer readable medium of claim 17, wherein the access request message contains a request for information stored at the secure computer network address.	Page 65: People and businesses who use IP networks tend to do so with the assumption that they can trust the origin and content of the data they work with, and that their transactions, if not secret, are reasonably private. Page 94: In theory, devices or services that authenticate using certificates must retrieve a current CRL before enabling access or establishing communication. Page 141: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs. End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider.

Petitioner Apple Inc. - Exhibit 1002, p. 692

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	Page 142: A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.
29. The computer-readable medium according to claim 17,	
wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;	Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel. Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of *name-to-address* and *address-to-name* mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or *resolve*) a name to an address (or vice versa) and a server-to-server update mechanism called a *zone transfer*. Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF *DNS Security* (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137). Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the *secure* IP address) in one that is routable from the given location. Page 191: 1. User ID a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com Page 243: *Domain Name Service*. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.
wherein sending the query message comprises sending the query message at the client computer;	Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel. Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses

Petitioner Apple Inc. - Exhibit 1002, p. 693

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	(such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of *name-to-address* and *address-to-name* mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or *resolve*) a name to an address (or vice versa) and a server-to-server update mechanism called a *zone transfer*. Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF *DNS Security* (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137). Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the *secure* IP address) in one that is routable from the given location. Page 191: 1. User ID a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com Page 243: *Domain Name Service*. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.
wherein receiving the response message comprises receiving the response message at the client computer,	Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel. Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of *name-to-address* and *address-to-name* mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or *resolve*) a name to an address (or vice versa) and a server-to-server update mechanism called a *zone transfer*. Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF *DNS Security* (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137) Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software

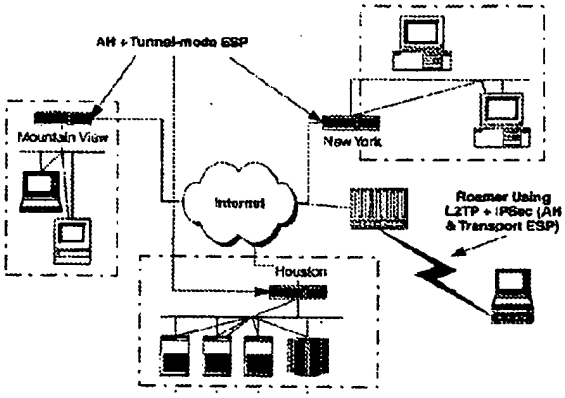
Petitioner Apple Inc. - Exhibit 1002, p. 694

7,188.180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the *secure* IP address) in one that is routable from the given location. Page 191: 1. User ID a. a fully qualified user name string (DNS), e.g., mozart@foo.bar.com Page 243: *Domain Name Service*. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.
wherein sending the access request message comprises sending the access request message at the client computer.	Page 65: People and businesses who use IP networks tend to do so with the assumption that they can trust the origin and content of the data they work with, and that their transactions, if not secret, are reasonably private. Page 94: In theory, devices or services that authenticate using certificates must retrieve a current CRL before enabling access or establishing communication. Page 141: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs. End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider. Page 142: A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.
30. The computer-readable medium according to claim 17, wherein the method is performed by a software module.	Page 133: Many network devices use *Trivial File Transfer Protocol* (TFTP) to retrieve new versions of software from a TFTP server (usually a UNIX host) and to upload copies of their running configurations, core dumps, error messages, or other diagnostics. Page 180: Integration of IPsec into the native IP implementation. This requires access to the IP source code and is applicable to both hosts and security gateways. Page 222: IPsec always has to figure out what the encapsulating IP header fields are. This is independent of where you insert IPsec and is intrinsic to the definition of IPsec. Therefore any IPsec implementation that is not integrated into an IP implementation must include code to construct the necessary IP headers (e.g., IP2):
31. The computer-readable medium according to claim 17, wherein the method is performed by a client computer.	Pages 141-142: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs. End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local

Petitioner Apple Inc. - Exhibit 1002, p. 695

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	service provider. A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network. Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the *secure* IP address) in one that is routable from the given location.
33. A data processing apparatus, comprising:	Pages 141-142: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs. End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider.

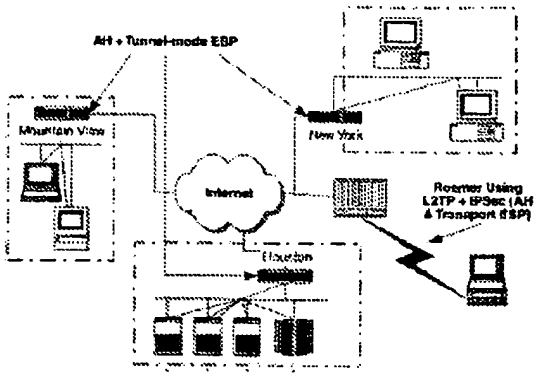
Petitioner Apple Inc. - Exhibit 1002, p. 696

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	 Figure 9.1 IPsec VPN.
a processor, and	Pages 103-104: Most current commercial IPsec products are software implementations on a general-purpose CPU with some hardware components to accelerate cryptographic operations. Software products have the advantage of being relatively easy to modify, but they can encounter memory constraints, processor restrictions, and arbitrary-seeming configuration limitations. Page 129: Host-based systems are software packages that scan traffic coming in to a particular end host. Intrusion detection is one of the few real-time security technologies that can be configured to adapt to the actual operating characteristics of a network and can also provide rapid, specific countermeasures in the event of a possible attack.
memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:	Page 2: The IPsec protocols were designed to clear the hit list of well-known security flaws in the current Internet Protocol version 4 (IPv4) and to provide a preemptive strike against these same flaws in its possible replacement, the Internet Protocol version 6 (IPv6). They provide standard, highly generalized, cryptographic security mechanisms for authentication, access control, confidentiality, data integrity, replay protection, and protection against traffic flow analysis. Page 9: As Dynamic Host Configuration Protocol (DHCP) becomes prevalent and people need access to data

Petitioner Apple Inc. - Exhibit 1002, p. 697

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	from more locations inside and outside your company, your security solutions will need to adapt to a dynamic IP network in order to authenticate users and enforce security principles. In the past, both users and IP addresses tended to be static. The average person might have had one address for his PC or workstation on the corporate LAN and another for his home SLIP or PPP connection. Today corporate users often drag their laptops around with them and obtain new addresses every time they restart their machines. They expect to work on business trips from airports, from hotels, or even from networks at other companies. Security perimeters can no longer work from static rules that associate a person with one or two IP addresses. Instead, they must rely on various user authentication technologies to identify users and their privileges, while also taking into account any additional constraints associated with a given user's current physical location. Page 83: Insert the ESP header, payload, and trailer (plus authentication/integrity data) directly after the IP header. (Note that in IPv6, the ESP data belongs after all of the hop-by-hop headers.) Pages 103-104: Most current commercial IPsec products are software implementations on a general-purpose CPU with some hardware components to accelerate cryptographic operations. Software products have the advantage of being relatively easy to modify, but they can encounter memory constraints, processor restrictions, and arbitrary-seeming configuration limitations. Page 129: Host-based systems are software packages that scan traffic coming in to a particular end host. Intrusion detection is one of the few real-time security technologies that can be configured to adapt to the actual operating characteristics of a network and can also provide rapid, specific countermeasures in the event of a possible attack. Page 140: Businesses generally deploy IPsec gateway-to-gateway (or network-to-network) as a secure alternative to a private WAN or leased-line connection. . . . . An extranet is an instance of a *virtual private network* (VPN), described in the section that follows. Because an extranet involves a trust relationship among entities that are not part of a single trust hierarchy, either each gateway needs to participate in each organization's PKI or each organization needs to deploy a PKI capable of cross-certifying portions of its trust hierarchy. Pages 141-142: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs. End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider. A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.

Petitioner Apple Inc. - Exhibit 1002, p. 698

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	 Figure 9.1 IPsec VPN.
receiving a secure domain name;	Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel. Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of *name-to-address* and *address-to-name* mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or *resolve*) a name to an address (or vice versa) and a server-to-server update mechanism called a *zone transfer*. Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF *DNS Security* (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see

Petitioner Apple Inc. - Exhibit 1002, p. 699

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	RFC 2065 and RFC 2137). Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the *secure* IP address) in one that is routable from the given location. Page 191: 1. User ID a. a fully qualified user name string (DNS), e.g., mozart@foo.bar.com Page 243: *Domain Name Service*. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.
sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;	Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel. Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of *name-to-address* and *address-to-name* mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or *resolve)* a name to an address (or vice versa) and a server to server update mechanism called a *zone transfer.* Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF *DNS Security* (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137). Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the *secure* IP address) in one that is routable from the given location. Page 191: 1. User ID a. a fully qualified user name string (DNS), e.g., mozart@foo.bar.com Page 243: *Domain Name Service*. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.

Petitioner Apple Inc. - Exhibit 1002, p. 700

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and	Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel. Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of *name-to-address* and *address-to-name* mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or *resolve*) a name to an address (or vice versa) and a server-to-server update mechanism called a *zone transfer*. Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF *DNS Security* (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137). Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the *secure* IP address) in one that is routable from the given location. Page 191: 1. User ID a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com Page 243: *Domain Name Service*. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.
sending an access request message to the secure computer network address using a virtual private network communication link.	Page 65: People and businesses who use IP networks tend to do so with the assumption that they can trust the origin and content of the data they work with, and that their transactions, if not secret, are reasonably private. Page 94: In theory, devices or services that authenticate using certificates must retrieve a current CRL before enabling access or establishing communication. Page 141: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs. End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider. Page 142: A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network

Petitioner Apple Inc. - Exhibit 1002, p. 701

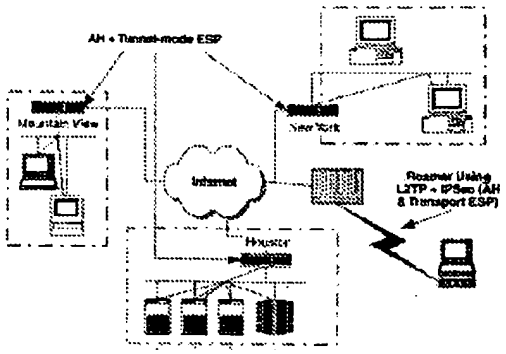
7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman Prior Art Reference
	over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.
35. The apparatus of claim 33, wherein the response message contains provisioning information for the virtual private network.	Page 121: RSVP is a signaling protocol used to negotiate in advance a hop-by-hop bandwidth reservation for specified traffic (Braden 1997). It does not carry data, but rather negotiates on behalf of an application. To request bandwidth, an RSVP-enabled application sends a PATH request toward its destination, including a traffic specification for the application and a request for some amount of bandwidth allocation. RSVP capable gateways reply back with RESV reservation responses. Application traffic then follows the signaling path across the network. RSVP arranges for only a unidirectional bandwidth allocation. It is designed to support applications that need significant available one-way bandwidth, such as streaming audio or video. If an application has significant bi- or multidirectional traffic requirements, each traffic originator must negotiate separately for bandwidth reservations.

Petitioner Apple Inc. - Exhibit 1002, p. 702

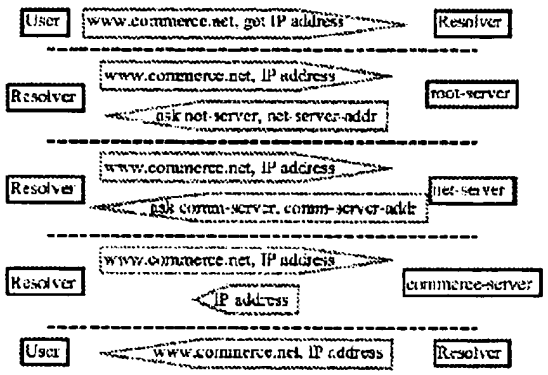
Appendix E
Citations to Exemplary Description in the Kaufman and Galvin References*

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
1. A method for accessing a secure computer network address, comprising steps of:	Kaufman, Page 2: The IPsec protocols were designed to clear the hit list of well-known security flaws in the current Internet Protocol version 4 (IPv4) and to provide a preemptive strike against these same flaws in its possible replacement, the Internet Protocol version 6 (IPv6). They provide standard, highly generalized, cryptographic security mechanisms for: authentication, access control, confidentiality, data integrity, replay protection, and protection against traffic flow analysis. Kaufman, Page 9: As Dynamic Host Configuration Protocol (DHCP) becomes prevalent and people need access to data from more locations inside and outside your company, your security solutions will need to adapt to a dynamic IP network in order to authenticate users and enforce security principles. In the past, both users and IP addresses tended to be static. The average person might have had one address for his PC or workstation on the corporate LAN and another for his home SLIP or PPP connection. Today corporate users often drag their laptops around with them and obtain new addresses every time they restart their machines. They expect to work on business trips from airports, from hotels, or even from networks at other companies. Security perimeters can no longer work from static rules that associate a person with one or two IP addresses. Instead, they must rely on various user authentication technologies to identify users and their privileges, while also taking into account any additional constraints associated with a given user's current physical location. Kaufman, Page 140: Businesses generally deploy IPsec gateway-to-gateway (or network-to-network) as a secure alternative to a private WAN or leased-line connection. . . . . An extranet is an instance of a virtual private network (VPN), described in the section that follows. Because an extranet involves a trust relationship among entities that are not part of a single trust hierarchy, either each gateway needs to participate in each organization's PKI or each organization needs to deploy a PKI capable of cross-certifying portions of its trust hierarchy. Kaufman, Pages 141-142: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs. End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider. A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.

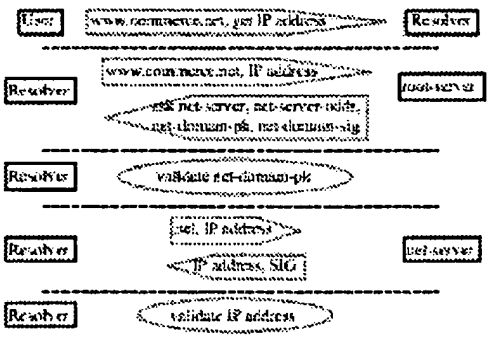
* - The cited passages are an indication of where in the Kaufman and Galvin references, at the very least, the claims find exemplary description. Requestor reserves the right to identify and demonstrate additional description if necessary or desirable.

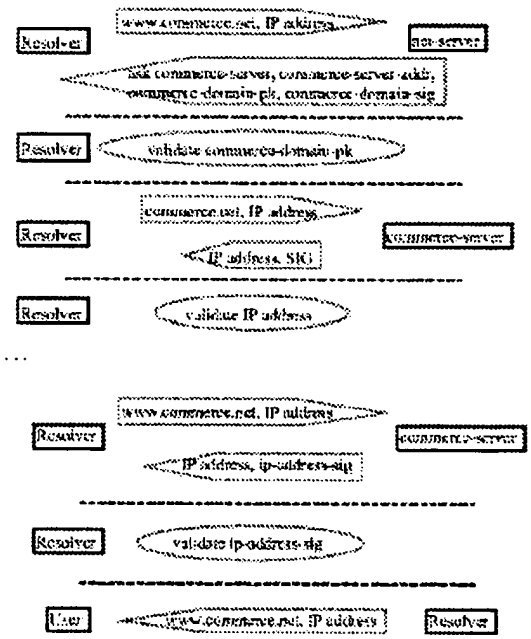
7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	 Figure 9.1 IPsec VPN. Kaufman, Page 200: The simplest form of management is manual management, in which a person manually configures each system with keying material and security association management data relevant to secure communication with other systems. Manual techniques are practical in small, static environments but they do not scale well. For example, a company could create a Virtual Private Network (VPN) using IPsec in security gateways at several sites. If the number of sites is small, and since all the sites come under the purview of a single administrative domain, this is likely to be a feasible context for manual management techniques. In this case, the security gateway might selectively protect traffic to and from other sites within the organization using a manually configured key, while not protecting traffic for other destinations.
receiving a secure domain name;	Kaufman, Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel. Kaufman, Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of *name-to-address* and *address-to-name* mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or *resolve*) a name to an address (or vice versa) and a server-to-server update mechanism called a *zone transfer*.

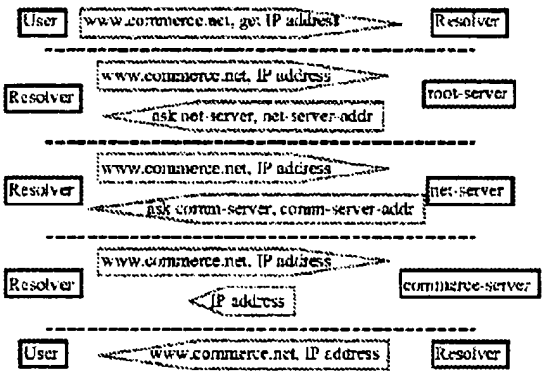
Petitioner Apple Inc. - Exhibit 1002, p. 704

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	Kaufman, Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF *DNS Security* (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137). Kaufman, Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the *secure* IP address) in one that is routable from the given location. Kaufman, Page 191: 1. User ID a. a fully qualified user name string (DNS), e.g., mozart@foo.bar.com Kaufman, Page 243: *Domain Name Service*. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.
sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;	Galvin § 2.2:  Galvin § 3: **3. Secure Domain Name System** Security enhancements for the DNS [9] have been drafted

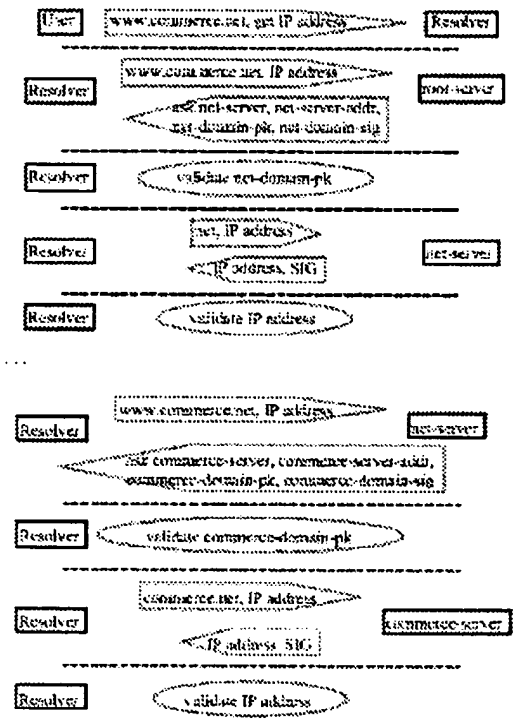
Petitioner Apple Inc. - Exhibit 1002, p. 705

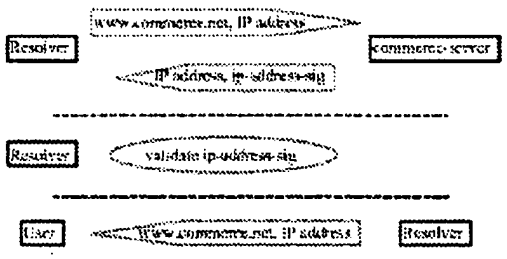
7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	and submitted for consideration as a Proposed Standard in the Internet. The enhancements include the security services of data integrity and data origin authentication, noting that a digital signature mechanism could support both services. The objective of the enhancements is to cryptographically bind domain names to their resources, i.e., digitally sign the resources records manages by the DNS. Galvin § 3.1.3: **Secure DNS Server Operation** The behavior of security aware servers is enhanced as follows . . . When responding to a query for data in a secure zone, both the resource record [e.g., DNS A record containing an IP address] and its corresponding signature record must be returned. Galvin § 3.2: [S]uppose a user application needs the IP address of the host www.commerce.net. The user application would invoke a local resolver that accepts responsibility for obtaining the IP address. Galvin § 3.2:  . . .

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	
receiving from the secure domain name service a response message containing the secure computer network address	Galvin § 2.2:

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
corresponding to the secure domain name; and	 Galvin § 3: **3. Secure Domain Name System** Security enhancements for the DNS [9] have been drafted and submitted for consideration as a Proposed Standard in the Internet. The enhancements include the security services of data integrity and data origin authentication, noting that a digital signature mechanism could support both services. The objective of the enhancements is to cryptographically bind domain names to their resources, i.e., digitally sign the resources records manages by the DNS. Galvin § 3.1.3: **Secure DNS Server Operation** The behavior of security aware servers is enhanced as follows . . . When responding to a query for data in a secure zone, both the resource record [e.g., DNS A record containing an IP address] and its corresponding signature record must be returned. Galvin § 3.2: [S]uppose a user application needs the IP address of the host www.commerce.net. The user application would invoke a local resolver that accepts responsibility for obtaining the IP address. Galvin § 3.2:

Petitioner Apple Inc. - Exhibit 1002, p. 708

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	
sending an access request message to the secure computer network address using a virtual private network communication link.	Kaufman, Page 65: People and businesses who use IP networks tend to do so with the assumption that they can trust the origin and content of the data they work with, and that their transactions, if not secret, are reasonably private. Kaufman, Page 94: In theory, devices or services that authenticate using certificates must retrieve a current CRL before enabling access or establishing communication. Kaufman, Page 141: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs. End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider. Kaufman, Page 142: A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.
4. The method according to claim 1, wherein the response message contains provisioning information for the virtual private network.	Kaufman, Page 121: RSVP is a signaling protocol used to negotiate in advance a hop-by-hop bandwidth reservation for specified traffic (Braden 1997). It does not carry data, but rather negotiates on behalf of an application. To request bandwidth, an RSVP-enabled application sends a PATH request toward its destination, including a traffic specification for the application and a request for some amount of bandwidth allocation. RSVP capable gateways reply back with RESV reservation responses. Application traffic then follows the signaling path across the network. RSVP arranges for only a unidirectional bandwidth allocation.

Petitioner Apple Inc. - Exhibit 1002, p. 710

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	It is designed to support applications that need significant available one-way bandwidth, such as streaming audio or video. If an application has significant bi- or multidirectional traffic requirements, each traffic originator must negotiate separately for bandwidth reservations.
10. The method according to claim 1, wherein the virtual private network includes the Internet.	Kaufman, Page 12: While you probably already know how the major parts of your network hang together, you probably do not have a comparable grasp of all the external connections that terminate somewhere inside your network perimeter. These connections may include lines leased to other organizations, departmental remote access servers and Internet connections, and analog or digital dial-up devices on individual networkconnected PCs. Kaufman, Pages 100-101: The standardization of a general-purpose secure transmission mechanism for IP has several advantages. It is very consistent with the overall layered design of the Internet, where protocols are intended to integrate without overt reference to or dependencies on one another. Kaufman, Page 126: Unfortunately, the places where IPsec might offer the most benefit are also the places where it is most difficult to deploy-in the core of the Internet and at peering points among multiple service providers. The challenge at administrative boundaries is not IPsec, but trust. Correct authentication of the IPsec peers requires either shared secrets-which are difficult to administer and almost impossible to scale--or some form of cross-certification among PKIs, which essentially requires (today) that all PKIs come from a single vendor.
12. The method of claim 1, wherein the access request message contains a request for information stored at the secure computer network address.	Kaufman, Page 65: People and businesses who use IP networks tend to do so with the assumption that they can trust the origin and content of the data they work with, and that their transactions, if not secret, are reasonably private. Kaufman, Page 94: In theory, devices or services that authenticate using certificates must retrieve a current CRL before enabling access or establishing communication. Kaufman, Page 141: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs. End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider. Kaufman, Page 142: A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.
13. The method of claim 1,	
wherein receiving the secure domain	Kaufman, Page 125: The technologies described in the following sections are among those vital to network

Petitioner Apple Inc. - Exhibit 1002, p. 711

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
name comprises receiving the secure domain name at a client computer from a user;	operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel. Kaufman, Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of *name-to-address* and *address-to-name* mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or *resolve*) a name to an address (or vice versa) and a server-to-server update mechanism called a *zone transfer*. Kaufman, Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF *DNS Security* (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137). Kaufman, Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the *secure* IP address) in one that is routable from the given location. Kaufman, Page 191: 1. User ID a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com Kaufman, Page 243: *Domain Name Service*. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.
wherein sending the query message comprises sending the query message at the client computer;	Kaufman, Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel. Kaufman, Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of *name-to-address* and *address-to-name* mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or *resolve*) a name to an address (or vice versa) and a server-to-server update mechanism called a *zone transfer*. Kaufman, Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF *DNS Security* (DNSSEC) working

Petitioner Apple Inc. - Exhibit 1002, p. 712

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137). Kaufman, Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the *secure* IP address) in one that is routable from the given location. Kaufman, Page 191: 1. User ID a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com Kaufman, Page 243: *Domain Name Service*. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.
wherein receiving the response message comprises receiving the response message at the client computer,	Kaufman, Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel. Kaufman, Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of *name-to-address* and *address-to-name* mappings. The two fundamental transactions conducted with the DNS are a client to server query to map (or *resolve*) a name to an address (or vice versa) and a server-to-server update mechanism called a *zone transfer*. Kaufman, Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF *DNS Security* (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137). Kaufman, Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the *secure* IP address) in one that is routable from the given location. Kaufman, Page 191: 1. User ID a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com Kaufman, Page 243: *Domain Name Service*. The protocol used to support the hierarchical resolution of host

Petitioner Apple Inc. - Exhibit 1002, p. 713

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	names to IP addresses (and vice versa) in the Internet.
wherein sending the access request message comprises sending the access request message at the client computer.	Kaufman, Page 65: People and businesses who use IP networks tend to do so with the assumption that they can trust the origin and content of the data they work with, and that their transactions, if not secret, are reasonably private. Kaufman, Page 94: In theory, devices or services that authenticate using certificates must retrieve a current CRL before enabling access or establishing communication. Kaufman, Page 141: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs. End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider. Kaufman, Page 142: A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.
14. The method of claim 1, performed by a software module.	Kaufman, Page 133. Many network devices use *Trivial File Transfer Protocol* (TFTP) to retrieve new versions of software from a TFTP server (usually a UNIX host) and to upload copies of their running configurations, core dumps, error messages, or other diagnostics. Kaufman, Page 180: Integration of IPsec into the native IP implementation. This requires access to the IP source code and is applicable to both hosts and security gateways. Kaufman, Page 222: IPsec always has to figure out what the encapsulating IP header fields are. This is independent of where you insert IPsec and is intrinsic to the definition of IPsec. Therefore any IPsec implementation that is not integrated into an IP implementation must include code to construct the necessary IP headers (e.g., IP2):
15. The method of claim 1, performed by a client computer.	Kaufman, Pages 141-142: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs. End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider. A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network. Kaufman, Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism

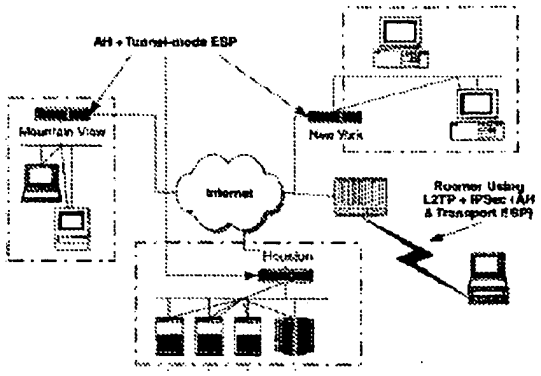
Petitioner Apple Inc. - Exhibit 1002, p. 714

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the *secure* IP address) in one that is routable from the given location.
17. A computer-readable storage medium, comprising:	Kaufman, Page 215: The use of IPsec imposes computational performance costs on the hosts or security gateways that implement these protocols. These costs are associated with the memory needed for IPsec code and data structures, and the computation of integrity check values, encryption and decryption, and added per-packet handling. The per-packet computational costs will be manifested by increased latency and, possibly, reduced throughput. Use of SA/key management protocols, especially ones that employ public key cryptography, also adds computational performance costs to use of IPsec. These per association computational costs will be manifested in terms of increased latency in association establishment. For many hosts, it is anticipated that software-based cryptography will not appreciably reduce throughput, but hardware may be required for security gateways (since they represent aggregation points), and for some hosts.
a storage area; and	Kaufman, Page 215. The use of IPsec imposes computational performance costs on the hosts or security gateways that implement these protocols. These costs are associated with the memory needed for IPsec code and data structures, and the computation of integrity check values, encryption and decryption, and added per-packet handling.
computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:	Kaufman, Page 2: The IPsec protocols were designed to clear the hit list of well-known security flaws in the current Internet Protocol version 4 (IPv4) and to provide a preemptive strike against these same flaws in its possible replacement, the Internet Protocol version 6 (IPv6). They provide standard, highly generalized, cryptographic security mechanisms for: authentication, access control, confidentiality, data integrity, replay protection, and protection against traffic flow analysis. Kaufman, Page 9: As Dynamic Host Configuration Protocol (DHCP) becomes prevalent and people need access to data from more locations inside and outside your company, your security solutions will need to adapt to a dynamic IP network in order to authenticate users and enforce security principles. In the past, both users and IP addresses tended to be static. The average person might have had one address for his PC or workstation on the corporate LAN and another for his home SLIP or PPP connection. Today corporate users often drag their laptops around with them and obtain new addresses every time they restart their machines. They expect to work on business trips from airports, from hotels, or even from networks at other companies. Security perimeters can no longer work from static rules that associate a person with one or two IP addresses. Instead, they must rely on various user authentication technologies to identify users and their privileges, while also taking into account any additional constraints associated with a given user's current physical location. Kaufman, Page 83: Insert the ESP header, payload, and trailer (plus authentication/integrity data) directly

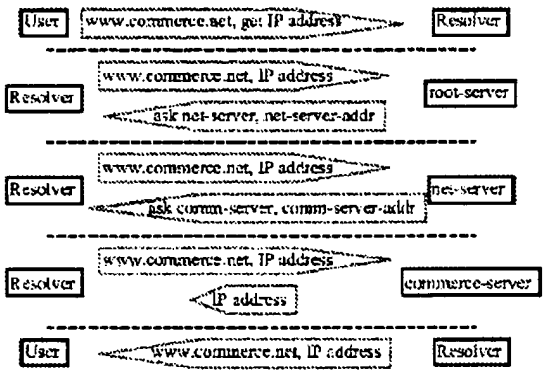
Petitioner Apple Inc. - Exhibit 1002, p. 715

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	after the IP header. (Note that in IPv6, the ESP data belongs after all of the hop-by-hop headers.) Kaufman, Pages 103-104: Most current commercial IPsec products are software implementations on a general-purpose CPU with some hardware components to accelerate cryptographic operations. Software products have the advantage of being relatively easy to modify, but they can encounter memory constraints, processor restrictions, and arbitrary-seeming configuration limitations. Kaufman, Page 129: Host-based systems are software packages that scan traffic coming in to a particular end host. Intrusion detection is one of the few real-time security technologies that can be configured to adapt to the actual operating characteristics of a network and can also provide rapid, specific countermeasures in the event of a possible attack. Kaufman, Page 140: Businesses generally deploy IPsec gateway-to-gateway (or network-to-network) as a secure alternative to a private WAN or leased-line connection. . . . . An extranet is an instance of a *virtual private network* (VPN), described in the section that follows. Because an extranet involves a trust relationship among entities that are not part of a single trust hierarchy, either each gateway needs to participate in each organization's PKI or each organization needs to deploy a PKI capable of cross-certifying portions of its trust hierarchy. Kaufman, Pages 141-142: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweigh: as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs. End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider. A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.

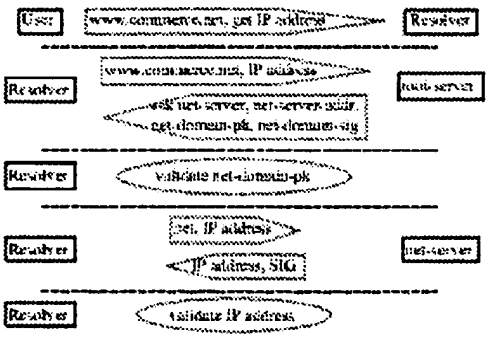
Petitioner Apple Inc. - Exhibit 1002, p. 716

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	 Figure 9.1 IPsec VPN.
receiving a secure domain name;	Kaufman, Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel. Kaufman, Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of *name-to-address* and *address-to-name* mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or *resolve)* a name to an address (or vice versa) and a server-to-server update mechanism called a *zone transfer.* Kaufman, Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF *DNS Security* (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137).

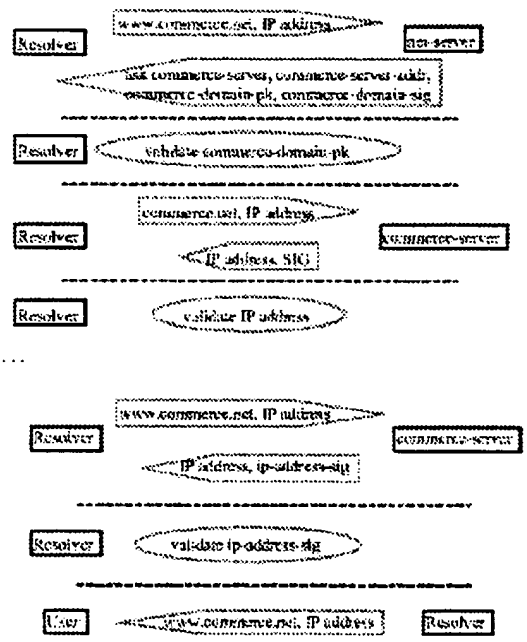
Petitioner Apple Inc. - Exhibit 1002, p. 717

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	Kaufman, Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the *secure* IP address) in one that is routable from the given location. Kaufman, Page 191: 1. User ID a. a fully qualified user name string {DNS}, e.g., mozart@foo.bar.com Kaufman, Page 243: *Domain Name Service.* The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.
sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain name;	Galvin § 2.2:  Galvin § 3: **3. Secure Domain Name System** Security enhancements for the DNS [9] have been drafted and submitted for consideration as a Proposed Standard in the Internet. The enhancements include the security services of data integrity and data origin authentication, noting that a digital signature mechanism could support both services. The objective of the enhancements is to cryptographically bind domain names to their resources, i.e., digitally sign the resources records manages by the DNS.

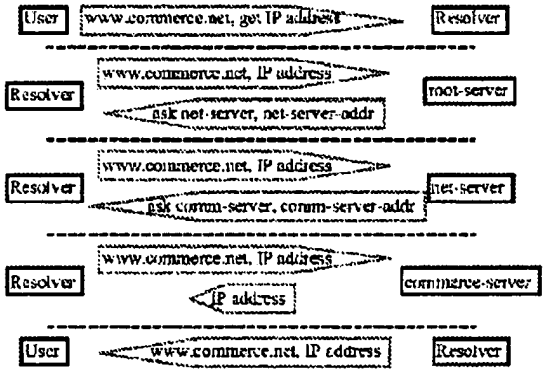
Petitioner Apple Inc. - Exhibit 1002, p. 718

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	Galvin § 3.1.3: **Secure DNS Server Operation** The behavior of security aware servers is enhanced as follows . . . When responding to a query for data in a secure zone, both the resource record [e.g., DNS A record containing an IP address] and its corresponding signature record must be returned. Galvin § 3.2: [S]uppose a user application needs the IP address of the host www.commerce.net. The user application would invoke a local resolver that accepts responsibility for obtaining the IP address. Galvin § 3.2:  . . .

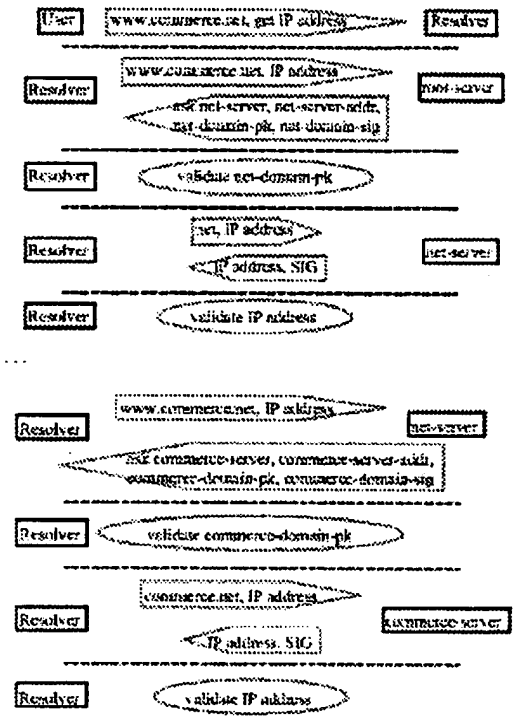
Petitioner Apple Inc. - Exhibit 1002, p. 719

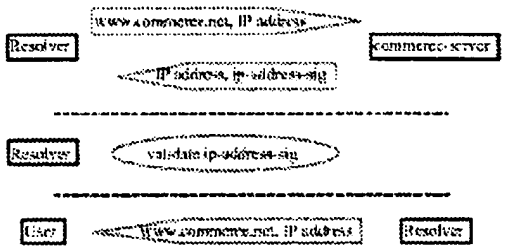
7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	
receiving from the domain name service a response message containing the secure computer network address	Galvin § 2.2:

Petitioner Apple Inc. - Exhibit 1002, p. 720

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
corresponding to the secure domain name; and	 Galvin § 3: **3. Secure Domain Name System** Security enhancements for the DNS [9] have been drafted and submitted for consideration as a Proposed Standard in the Internet. The enhancements include the security services of data integrity and data origin authentication, noting that a digital signature mechanism could support both services. The objective of the enhancements is to cryptographically bind domain names to their resources, i.e., digitally sign the resources records unanages by the DNS. Galvin § 3.1.3: **Secure DNS Server Operation** The behavior of security aware servers is enhanced as follows . . . When responding to a query for data in a secure zone, both the resource record [*e.g.*, DNS A record containing an IP address] and its corresponding signature record must be returned. Galvin § 3.2: [S]uppose a user application needs the IP address of the host www.commerce.net. The user application would invoke a local resolver that accepts responsibility for obtaining the IP address. Galvin § 3.2:

Petitioner Apple Inc. - Exhibit 1002, p. 721

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	
sending an access request message to the secure computer network address using a virtual private network communication link.	Kaufman, Page 65: People and businesses who use IP networks tend to do so with the assumption that they can trust the origin and content of the data they work with, and that their transactions, if not secret, are reasonably private. Kaufman, Page 94: In theory, devices or services that authenticate using certificates must retrieve a current CRL before enabling access or establishing communication. Kaufman, Page 141: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs. End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider. Kaufman, Page 142: A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.
20. The computer-readable medium according to claim 17, wherein the response message contains provisioning information for the virtual private network.	Kaufman, Page 121: RSVP is a signaling protocol used to negotiate in advance a hop-by-hop bandwidth reservation for specified traffic (Braden 1997). It does not carry data, but rather negotiates on behalf of an application. To request bandwidth, an RSVP-enabled application sends a PATH request toward its destination, including a traffic specification for the application and a request for some amount of bandwidth allocation. RSVP capable gateways reply back with RESV reservation responses. Application traffic then follows the signaling path across the network. RSVP arranges for only a unidirectional bandwidth allocation.

Petitioner Apple Inc. - Exhibit 1002, p. 723

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	It is designed to support applications that need significant available one-way bandwidth, such as streaming audio or video. If an application has significant bi- or multidirectional traffic requirements, each traffic originator must negotiate separately for bandwidth reservations.
26. The computer-readable medium according to claim 17, wherein the virtual private network includes the Internet.	Kaufman, Page 12: While you probably already know how the major parts of your network hang together, you probably do not have a comparable grasp of all the external connections that terminate somewhere inside your network perimeter. These connections may include lines leased to other organizations, departmental remote access servers and Internet connections, and analog or digital dial-up devices on individual networkconnected PCs. Kaufman, Pages 100-101: The standardization of a general-purpose secure transmission mechanism for IP has several advantages. It is very consistent with the overall layered design of the Internet, where protocols are intended to integrate without overt reference to or dependencies on one another. Kaufman, Page 126: Unfortunately, the places where IPsec might offer the most benefit are also the places where it is most difficult to deploy-in the core of the Internet and at peering points among multiple service providers. The challenge at administrative boundaries is not IPsec, but trust. Correct authentication of the IPsec peers requires either shared secrets-which are difficult to administer and almost impossible to scale--or some form of cross-certification among PKIs, which essentially requires (today) that all PKIs come from a single vendor.
28. The computer readable medium of claim 17, wherein the access request message contains a request for information stored at the secure computer network address.	Kaufman, Page 65: People and businesses who use IP networks tend to do so with the assumption that they can trust the origin and content of the data they work with, and that their transactions, if not secret, are reasonably private. Kaufman, Page 94: In theory, devices or services that authenticate using certificates must retrieve a current CRL before enabling access or establishing communication. Kaufman, Page 141: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs. End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider. Kaufman, Page 142: A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.
29. The computer-readable medium according to claim 17,	

Petitioner Apple Inc. - Exhibit 1002, p. 724

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;	Kaufman, Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel. Kaufman, Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of *name-to-address* and *address-to-name* mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or *resolve)* a name to an address (or vice versa) and a server-to-server update mechanism called a *zone transfer.* Kaufman, Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF *DNS Security* (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137). Kaufman, Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the *secure* IP address) in one that is routable from the given location. Kaufman, Page 191: 1. User ID a. a fully qualified user name string (DNS), e.g., mozart@foo.bar.com Kaufman, Page 243: *Domain Name Service.* The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.
wherein sending the query message comprises sending the query message at the client computer;	Kaufman, Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel. Kaufman, Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of *name-to-address* and *address-to-name* mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or *resolve)* a name to an address (or vice versa) and a server-to-server update mechanism called a *zone transfer.* Kaufman, Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and

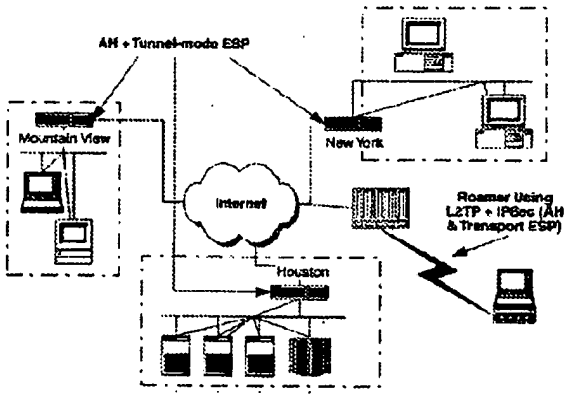
Petitioner Apple Inc. - Exhibit 1002, p. 725

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	malicious meddling can divert email, Web traffic, and more. The IETF *DNS Security* (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137). Kaufman, Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the *secure* IP address) in one that is routable from the given location. Kaufman, Page 191: 1. User ID a. a fully qualified user name string (DNS), e.g., mozart@foo.bar.com Kaufman, Page 243: *Domain Name Service*. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.
wherein receiving the response message comprises receiving the response message at the client computer,	Kaufman, Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel. Kaufman, Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of *name to address* and *address to name* mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or *resolve*) a name to an address (or vice versa) and a server-to-server update mechanism called a *zone transfer*. Kaufman, Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF *DNS Security* (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137). Kaufman, Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the *secure* IP address) in one that is routable from the given location. Kaufman, Page 191: 1. User ID a. a fully qualified user name string (DNS), e.g., mozart@foo.bar.com

Petitioner Apple Inc. - Exhibit 1002, p. 726

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	Kaufman, Page 243: *Domain Name Service*. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.
wherein sending the access request message comprises sending the access request message at the client computer.	Kaufman, Page 65: People and businesses who use IP networks tend to do so with the assumption that they can trust the origin and content of the data they work with, and that their transactions, if not secret, are reasonably private. Kaufman, Page 94: In theory, devices or services that authenticate using certificates must retrieve a current CRL before enabling access or establishing communication. Kaufman, Page 141: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs. End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider. Kaufman, Page 142: A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.
30. The computer-readable medium according to claim 17, wherein the method is performed by a software module.	Kaufman, Page 133: Many network devices use *Trivial File Transfer Protocol* (TFTP) to retrieve new versions of software from a TFTP server (usually a UNIX host) and to upload copies of their running configurations, core dumps, error messages, or other diagnostics. Kaufman, Page 180: Integration of IPsec into the native IP implementation. This requires access to the IP source code and is applicable to both hosts and security gateways. Kaufman, Page 222: IPsec always has to figure out what the encapsulating IP header fields are. This is independent of where you insert IPsec and is intrinsic to the definition of IPsec. Therefore any IPsec implementation that is not integrated into an IP implementation must include code to construct the necessary IP headers (e.g., IP2):
31. The computer-readable medium according to claim 17, wherein the method is performed by a client computer.	Kaufman, Pages 141-142: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs. End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider. A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.

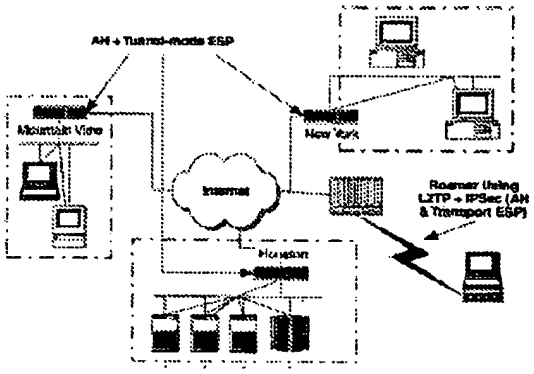
Petitioner Apple Inc. - Exhibit 1002, p. 727

7,188.180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	Kaufman, Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the *secure* IP address) in one that is routable from the given location.
33. A data processing apparatus comprising:	Kaufman, Pages 141-142: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweigh: as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs. End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider.  Figure 9.1 IPsec VPN

Petitioner Apple Inc. - Exhibit 1002, p. 728

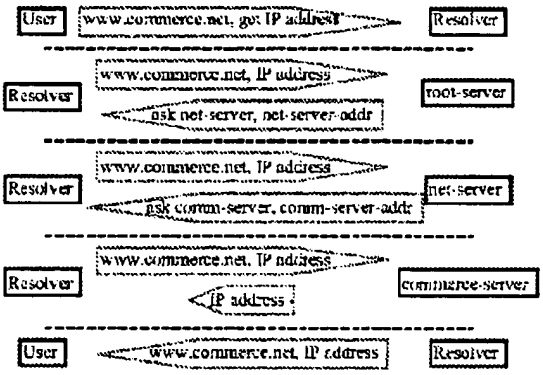
7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
a processor, and	Kaufman, Pages 103-104: Most current commercial IPsec products are software implementations on a general-purpose CPU with some hardware components to accelerate cryptographic operations. Software products have the advantage of being relatively easy to modify, but they can encounter memory constraints, processor restrictions, and arbitrary-seeming configuration limitations. Kaufman, Page 129: Host-based systems are software packages that scan traffic coming in to a particular end host. Intrusion detection is one of the few real-time security technologies that can be configured to adapt to the actual operating characteristics of a network and can also provide rapid, specific countermeasures in the event of a possible attack.
memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:	Kaufman, Page 2: The IPsec protocols were designed to clear the hit list of well-known security flaws in the current Internet Protocol version 4 (IPv4) and to provide a preemptive strike against these same flaws in its possible replacement, the Internet Protocol version 6 (IPv6). They provide standard, highly generalized, cryptographic security mechanisms for authentication, access control, confidentiality, data integrity, replay protection, and protection against traffic flow analysis. Kaufman, Page 9: As Dynamic Host Configuration Protocol (DHCP) becomes prevalent and people need access to data from more locations inside and outside your company, your security solutions will need to adapt to a dynamic IP network in order to authenticate users and enforce security principles. In the past, both users and IP addresses tended to be static. The average person might have had one address for his PC or workstation on the corporate LAN and another for his home SLIP or PPP connection. Today corporate users often drag their laptops around with them and obtain new addresses every time they restart their machines. They expect to work on business trips from airports, from hotels, or even from networks at other companies. Security perimeters can no longer work from static rules that associate a person with one or two IP addresses. Instead, they must rely on various user authentication technologies to identify users and their privileges, while also taking into account any additional constraints associated with a given user's current physical location. Kaufman, Page 83: Insert the ESP header, payload, and trailer (plus authentication/integrity data) directly after the IP header. (Note that in IPv6, the ESP data belongs after all of the hop-by-hop headers.) Kaufman, Pages 103-104: Most current commercial IPsec products are software implementations on a general-purpose CPU with some hardware components to accelerate cryptographic operations. Software products have the advantage of being relatively easy to modify, but they can encounter memory constraints, processor restrictions, and arbitrary-seeming configuration limitations. Kaufman, Page 129: Host-based systems are software packages that scan traffic coming in to a particular end host. Intrusion detection is one of the few real-time security technologies that can be configured to adapt to the actual operating characteristics of a network and can also provide rapid, specific countermeasures in the event of a possible attack. Kaufman, Page 140: Businesses generally deploy IPsec gateway-to-gateway (or network-to-network) as a secure alternative to a private WAN or leased-line connection. . . . .

Petitioner Apple Inc. - Exhibit 1002, p. 729

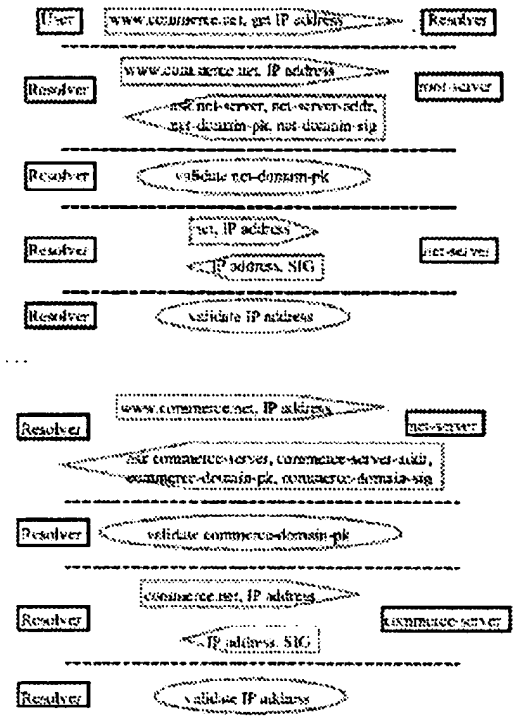
7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	An extranet is an instance of a *virtual private network* (VPN), described in the section that follows. Because an extranet involves a trust relationship among entities that are not part of a single trust hierarchy, either each gateway needs to participate in each organization's PKI or each organization needs to deploy a PKI capable of cross-certifying portions of its trust hierarchy. Kaufman, Pages 141-142: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweigh: as a separate IF addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs. End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider. A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.  Figure 9.1 IPsec VPN.

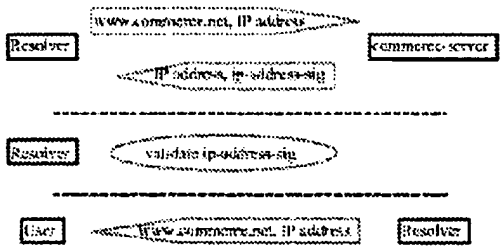
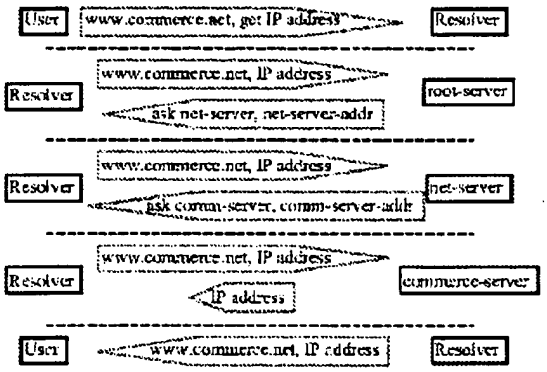
7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
receiving a secure domain name;	Kaufman, Page 125: The technologies described in the following sections are among those vital to network operation. If either IP routing or DNS fails, it is essentially a network down situation: The end user's experience is as dramatic as if you cut his connection with an axe. If you deploy IPsec in a gateway scenario, you will almost always need to punch explicit holes in your IPsec topology to ensure that routing information and DNS transactions do not get black holed in an encrypted tunnel. Kaufman, Page 127: The DNS is the basic mechanism used to translate between human comprehensible addresses (such as www.wiley.com) and IP network addresses (such as 10.235.134.17). It is a hierarchical system that allows very granular local control of *name-to-address* and *address-to-name* mappings. The two fundamental transactions conducted with the DNS are a client-to-server query to map (or *resolve*) a name to an address (or vice versa) and a server-to-server update mechanism called a *zone transfer*. Kaufman, Page 128: The integrity of the DNS is vital to the operation of the Internet and of any normal IP network. Accidental corruption of DNS information has caused spectacular meltdowns in the past, and malicious meddling can divert email, Web traffic, and more. The IETF *DNS Security* (DNSSEC) working group has developed several standards and draft recommendations for security mechanisms specific to the DNS (see RFC 2065 and RFC 2137). Kaufman, Pages 143-144: Dynamic Host Configuration Protocol (DHCP) is a nearly ubiquitous mechanism for address management for internal and remote IP systems on large IP networks. Unfortunately, DHCP can wreak havoc if IPsec end hosts are required to have invariant addresses. One solution, if supported by your software vendor, would be to use ESP tunnel mode from the end host and assign a permanent, internal IP address to use for identification during key exchange. The external IP address could be assigned by DHCP. All IPsec secure communications would then utilize tunnel-mode ESP and wrap the internal IP packet (using the *secure* IP address) in one that is routable from the given location. Kaufman, Page 191: 1. User ID a. a fully qualified user name string (DNS), e.g., mozart@foo.bar.com Kaufman, Page 243: *Domain Name Service*. The protocol used to support the hierarchical resolution of host names to IP addresses (and vice versa) in the Internet.
sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;	Galvin § 2.2:

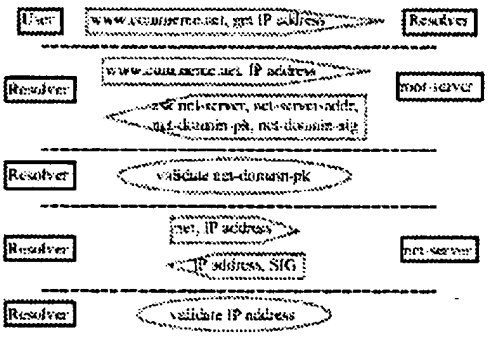
Petitioner Apple Inc. - Exhibit 1002, p. 731

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	 Galvin § 3: **3. Secure Domain Name System** Security enhancements for the DNS [9] have been drafted and submitted for consideration as a Proposed Standard in the Internet. The enhancements include the security services of data integrity and data origin authentication, noting that a digital signature mechanism could support both services. The objective of the enhancements is to cryptographically bind domain names to their resources, i.e., digitally sign the resources records manages by the DNS. Galvin § 3.1.3: **Secure DNS Server Operation** The behavior of security aware servers is enhanced as follows . . . When responding to a query for data in a secure zone, both the resource record [e.g., DNS A record containing an IP address] and its corresponding signature record must be returned. Galvin § 3.2: [S]uppose a user application needs the IP address of the host www.commerce.net. The user application would invoke a local resolver that accepts responsibility for obtaining the IP address. Galvin § 3.2:

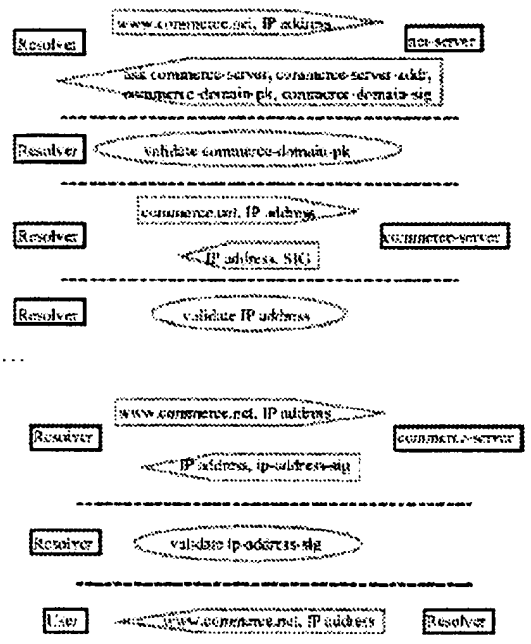
Petitioner Apple Inc. - Exhibit 1002, p. 732

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	

7,188.180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	
receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and	Galvin § 2.2:  Galvin § 3: **3. Secure Domain Name System** Security enhancements for the DNS [9] have been drafted and submitted for consideration as a Proposed Standard in the Internet. The enhancements include the

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	security services of data integrity and data origin authentication, noting that a digital signature mechanism could support both services. The objective of the enhancements is to cryptographically bind domain names to their resources, i.e., digitally sign the resources records manages by the DNS. Galvin § 3.1.3: **Secure DNS Server Operation** The behavior of security aware servers is enhanced as follows . . . When responding to a query for data in a secure zone, both the resource record [*e.g.*, DNS A record containing an IP address] and its corresponding signature record must be returned. Galvin § 3.2: [S]uppose a user application needs the IP address of the host www.commerce.net. The user application would invoke a local resolver that accepts responsibility for obtaining the IP address. Galvin § 3.2:  . . .

Petitioner Apple Inc. - Exhibit 1002, p. 735

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
	
sending an access request message to the secure computer network address using a virtual private network	Kaufman, Page 65: People and businesses who use IP networks tend to do so with the assumption that they can trust the origin and content of the data they work with, and that their transactions, if not secret, are reasonably private.

7,188,180 Claim Elements	Description for Claimed Elements in the Kaufman and Galvin Prior Art References
communication link.	Kaufman, Page 94: In theory, devices or services that authenticate using certificates must retrieve a current CRL before enabling access or establishing communication. Kaufman, Page 141: A VPN, in its broadest interpretation, is a private logical network that uses a shared physical medium. The privacy element can be as lightweight as a separate IP addressing scheme or as heavyweight as tunnel-mode AH+ESP with 3DES. Frame relay networks, dial-up networks, and IPsec networks are all instances of VPNs. End host-to-gateway IPsec installations provide an attractive, relatively low-cost mechanism for businesses to provide their telecommuting and mobile employees with secure remote access through a local service provider. Kaufman, Page 142: A layer 2 tunneling protocol allows a host to establish a virtual presence on a corporate network over a remote connection. Because the tunnel is at layer 2 and terminates on a home gateway, the remote host can receive an IP address internal to its home network.
35. The apparatus of claim 33, wherein the response message contains provisioning information for the virtual private network.	Kaufman, Page 121: RSVP is a signaling protocol used to negotiate in advance a hop-by-hop bandwidth reservation for specified traffic (Braden 1997). It does not carry data, but rather negotiates on behalf of an application. To request bandwidth, an RSVP-enabled application sends a PATH request toward its destination, including a traffic specification for the application and a request for some amount of bandwidth allocation. RSVP capable gateways reply back with RESV reservation responses. Application traffic then follows the signaling path across the network. RSVP arranges for only a unidirectional bandwidth allocation. It is designed to support applications that need significant available one-way bandwidth, such as streaming audio or video. If an application has significant bi- or multidirectional traffic requirements, each traffic originator must negotiate separately for bandwidth reservations.

Petitioner Apple Inc. - Exhibit 1002, p. 737

Appendix F
Citations to Exemplary Description in the Gauntlet Admin Guide Reference*

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference
1. A method for accessing a secure computer network address, comprising steps of:	Page 1-9: The proxies also check to determine if the request is permitted for the destination. For some services, the proxies can perform the additional step of authenticating the user. This helps verify that users are who they say they are. The proxy then passes the request to the appropriate machine on the other side of the firewall using the standard protocol for that service. Page 18-1: You are concerned about the security of communications on the Internet between your company and your client site. You can use the Point-To-Point Tunneling (PPTP) protocol to provide secure transfer between your site and your client site. The PPTP proxy included with the Gauntlet firewall allows you to tunnel PPTP traffic through the firewall. This chapter explains how the PPTP proxy works and how to configure it. The typical use of PPTP involves remote PPTP clients on the untrusted network accessing a local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server. Page 28-2: For example, consider the situation of a user, John, working at a client site (blaze.clientsite.com) who needs information stored on a machine at work (dimension.yoyodine.com). When John tries to FTP to dimension, which is within the perimeter, he must authenticate at the firewall (fire-out.yoyodyne.com). The FTP proxy then prompts John for his authentication information (user name and password), which it verifies against the information in the user authentication database. If John provided the proper information, and his account is not disabled, the proxy provides a prompt. John can then connect to dimension on the inside network. Page 30-5: When nodes on these private networks attempt to communicate with each other (via a VPN) or over a public network (such as the Internet), the reusable (non-routable) IP addresses must be translated to unique, globally routable IP addresses.

* - The cited passages are an indication of where in the Gauntlet reference, at the very least, the claims find exemplary description. Requestor reserves the right to identify and demonstrate additional description if necessary or desirable.

<table>
<tr><th>7,188,180 Claim Elements</th><th>Description for Claimed Elements in the Gauntlet Prior Art Reference</th></tr>
<tr><td>receiving a secure domain name;</td><td>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.
Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that policy or proxy, the firewall passes on the request.
Page 5-2: The firewall must perform additional processing steps to convert the address that is in the packet and the hostname that is in the configuration rule to the same format so that it can compare the values, so performance may be slow.
If you deny by host name, the proxy must use DNS to map the source or destination address (in the packet) into a host name.
Page 5-4:
<table><tr><th>Parameters</th><th>Enter</th></tr><tr><td>IP Address & Mask</td><td>Enter the IP address of the machine to which you want to permit or deny access.

Note: You cannot use the asterisk (*) wildcard in this field.</td></tr><tr><td>or Hostname</td><td>Enter a hostname to which you want to permit or deny access, such as www.bigu.edu.

Note: You cannot use the asterisk (*) wildcard in this field.</td></tr></table>Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing.
Page G-1:
domain name system (DNS) — The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.</td></tr>
</table>

Petitioner Apple Inc. - Exhibit 1002, p. 739

<table>
<tr><th>7,188,180 Claim Elements</th><th>Description for Claimed Elements in the Gauntlet Prior Art Reference</th></tr>
<tr><td>sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;</td><td>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.
Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that policy or proxy, the firewall passes on the request.
Page 5-4:
<table><tr><th>Parameters</th><th>Enter</th></tr><tr><td>IP Address & Mask</td><td>Enter the IP address of the machine to which you want to permit or deny access.

Note: You cannot use the asterisk (*) wildcard in this field.</td></tr><tr><td>or Hostname</td><td>Enter a hostname to which you want to permit or deny access, such as www.bigu.edu.

Note: You cannot use the asterisk (*) wildcard in this field.</td></tr></table>Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing.
Page G-1:
domain name system (DNS) — The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.</td></tr>
</table>

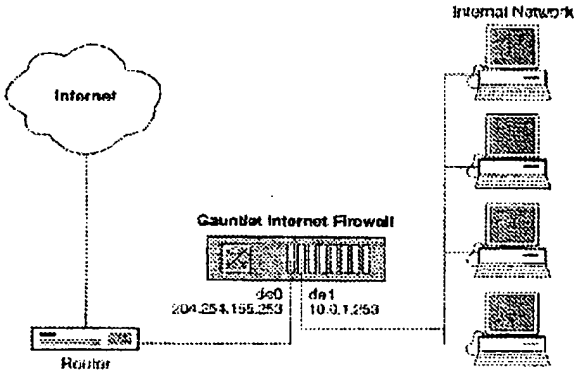
Petitioner Apple Inc. - Exhibit 1002, p. 740

<table>
<tr><th>7,188,180 Claim Elements</th><th>Description for Claimed Elements in the Gauntlet Prior Art Reference</th></tr>
<tr><td>receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</td><td>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.
Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that policy or proxy, the firewall passes on the request.
Page 5-4:
<table>
<tr><th>Parameters</th><th>Enter</th></tr>
<tr><td>IP Address & Mask</td><td>Enter the IP address of the machine to which you want to permit or deny access.

Note: You cannot use the asterisk (*) wildcard in this field.</td></tr>
<tr><td>or Hostname</td><td>Enter a hostname to which you want to permit or deny access, such as www.bigu.edu.

Note: You cannot use the asterisk (*) wildcard in this field.</td></tr>
</table>
Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing.
Page G-1:
domain name system (DNS) — The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.</td></tr>
</table>

Petitioner Apple Inc. - Exhibit 1002, p. 741

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference
sending an access request message to the secure computer network address using a virtual private network communication link.	Page 1-7:  Page 18-1: You are concerned about the security of communications on the Internet between your company and your client site. You can use the Point-To-Point Tunneling (PPTP) protocol to provide secure transfer between your site and your client site. The PPTP proxy included with the Gauntlet firewall allows you to tunnel PPTP traffic through the firewall. This chapter explains how the PPTP proxy works and how to configure it. The typical use of PPTP involves remote PPTP clients on the untrusted network accessing a local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.
4. The method according to claim 1, wherein the response message contains provisioning information for the virtual private network.	Page 1-8. Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall. Page 5-4:

Petitioner Apple Inc. - Exhibit 1002, p. 742

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference

Parameters	Enter
IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. **Note:** You cannot use the asterisk (*) wildcard in this field.
or Hostname	Enter a hostname to which you want to permit or deny access, such as www.bigu.edu. **Note:** You cannot use the asterisk (*) wildcard in this field.

Pages 18-1 - 18-4: You are concerned about the security of communications on the Internet between your company and your client site. You can use the Point-To-Point Tunneling (PPTP) protocol to provide secure transfer between your site and your client site. The PPTP proxy included with the Gauntlet firewall allows you to tunnel PPTP traffic through the firewall. This chapter explains how the PPTP proxy works and how to configure it.

. . . .

Configuring the firewall to allow PPTP traffic involves several steps that must be coordinated. You must configure:

The PPTP proxy to allow TCP Control connections
Policies to allow the PPTP proxy
Packet Screening to allow IP Data connections
Packet Screening to absorb incoming TCP Control connections
Routing on the PPTP client and server machines

. . . .

Configuring the PPTP Proxy

PPTP tunnels are initiated by client machines. Perform the following steps to configure the PPTP proxy to allow connections from all the desired clients.

. . . .

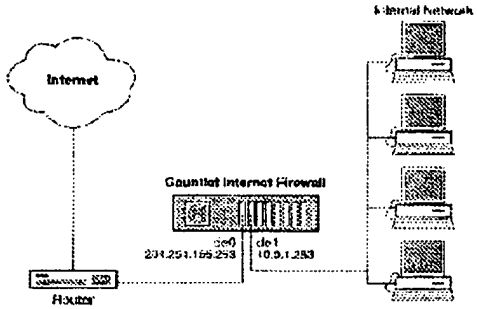
5. Provide information about the hosts that will communicate through the PPTP proxy.

- Enter the IP address and mask or the host name of the machine or network sending PPTP requests. The asterisk wildcard (*) is valid in host names.
- Enter the IP address or host name of the hosts to which the PPTP proxy should connect.
- Enter the port number of the remote host to which the PPTP proxy sends requests. The default port is 1723.
- If desired, enter a description for your rule.

Page G-1:

domain name system (DNS) The online distributed database system used to map human-readable

Petitioner Apple Inc. - Exhibit 1002, p. 743

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference
	machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.
10. The method according to claim 1, wherein the virtual private network includes the Internet.	Page 1-7:  Page 30-5: When nodes on these private networks attempt to communicate with each other (via a VPN) or over a public network (such as the Internet), the reusable (non-routable) IP addresses must be translated to unique, globally routable IP addresses.
12. The method of claim 1, wherein the access request message contains a request for information stored at the secure computer network address.	Page 18-1: You are concerned about the security of communications on the Internet between your company and your client site. You can use the Point-To-Point Tunneling (PPTP) protocol to provide secure transfer between your site and your client site. The PPTP proxy included with the Gauntlet firewall allows you to tunnel PPTP traffic through the firewall. This chapter explains how the PPTP proxy works and how to configure it. The typical use of PPTP involves remote PPTP clients on the untrusted network accessing a local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.
13. The method of claim 1,	
wherein receiving the secure domain	Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to

Petitioner Apple Inc. - Exhibit 1002, p. 744

<table>
<tr><th>7,188,180 Claim Elements</th><th>Description for Claimed Elements in the Gauntlet Prior Art Reference</th></tr>
<tr><td>name comprises receiving the secure domain name at a client computer from a user;</td><td>the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.
Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that policy or proxy, the firewall passes on the request.
Page 5-2: The firewall must perform additional processing steps to convert the address that is in the packet and the hostname that is in the configuration rule to the same format so that it can compare the values, so performance may be slow.
If you deny by host name, the proxy must use DNS to map the source or destination address (in the packet) into a host name.
Page 5-4:
<table><tr><th>Parameters</th><th>Enter</th></tr><tr><td>IP Address & Mask</td><td>Enter the IP address of the machine to which you want to permit or deny access.

Note: You cannot use the asterisk (*) wildcard in this field.</td></tr><tr><td>or Hostname</td><td>Enter a hostname to which you want to permit or deny access, such as www.bigu.edu.

Note: You cannot use the asterisk (*) wildcard in this field.</td></tr></table>Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodync.com) to the firewall (firc-out.yoyodync.com) itself for processing.
Page G-1:
<table><tr><td>domain name system (DNS)</td><td>The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.</td></tr></table></td></tr>
<tr><td>wherein sending the query message comprises sending the query message at the client computer;</td><td>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.
Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that</td></tr>
</table>

Petitioner Apple Inc. - Exhibit 1002, p. 745

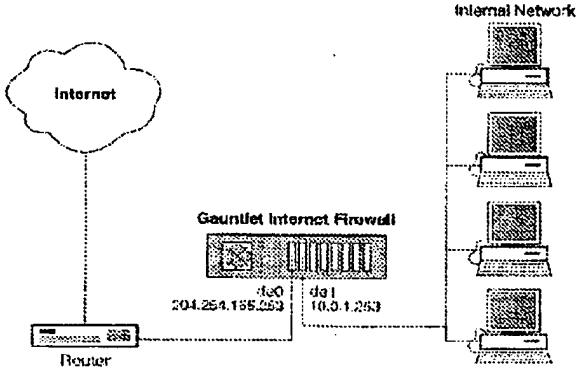
<table>
<tr><th>7,188,180 Claim Elements</th><th>Description for Claimed Elements in the Gauntlet Prior Art Reference</th></tr>
<tr><td></td><td>policy or proxy, the firewall passes on the request.
Page 5-4:<table><tr><th>Parameters</th><th>Enter</th></tr><tr><td>IP Address & Mask</td><td>Enter the IP address of the machine to which you want to permit or deny access.

Note: You cannot use the asterisk (*) wildcard in this field.</td></tr><tr><td>or Hostname</td><td>Enter a hostname to which you want to permit or deny access, such as www.bigu.edu.

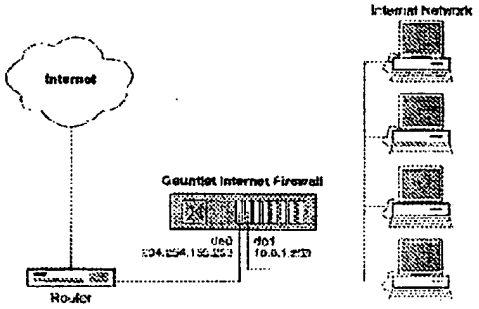
Note: You cannot use the asterisk (*) wildcard in this field.</td></tr></table>Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing.
Page G-1:<table><tr><td>domain name system (DNS)</td><td>The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.</td></tr></table></td></tr>
<tr><td>wherein receiving the response message comprises receiving the response message at the client computer,</td><td>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.
Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that policy or proxy, the firewall passes on the request.
Page 5-4:<table><tr><th>Parameters</th><th>Enter</th></tr><tr><td>IP Address & Mask</td><td>Enter the IP address of the machine to which you want to permit or deny access.

Note: You cannot use the asterisk (*) wildcard in this field.</td></tr><tr><td>or Hostname</td><td>Enter a hostname to which you want to permit or deny access, such as www.bigu.edu.</td></tr></table></td></tr>
</table>

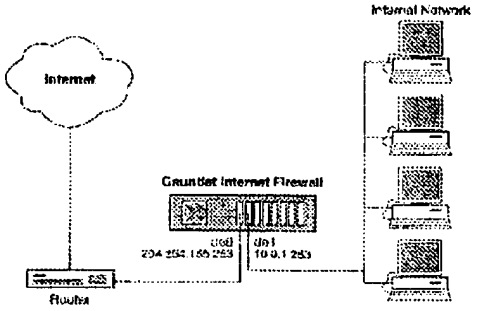
Petitioner Apple Inc. - Exhibit 1002, p. 746

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference
	Note: You cannot use the asterisk (*) wildcard in this field. Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing. Page G-1: domain name system (DNS) — The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.
wherein sending the access request message comprises sending the access request message at the client computer.	Page 1-7:  Page 18-1: You are concerned about the security of communications on the Internet between your company and your client site. You can use the Point-To-Point Tunneling (PPTP) protocol to provide secure transfer between your site and your client site. The PPTP proxy included with the Gauntlet firewall allows you to tunnel PPTP traffic through the firewall. This chapter explains how the PPTP proxy works and how to configure it. The typical use of PPTP involves remote PPTP clients on the untrusted network accessing a local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops

Petitioner Apple Inc. - Exhibit 1002, p. 747

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference
	can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.
14. The method of claim 1, performed by a software module.	*See* claim 1, which is performed by software at the client computer (e.g., Internet browser, Windows NT, other software the user may use). Page 18-1: The typical use of PPTP involves remote PPTP clients on the untrusted network accessing a local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.
15. The method of claim 1, performed by a client computer.	*See* claim 1, which is performed by software at the client computer (e.g., Internet browser, Windows NT, other software the user may use). Page 18-1: The typical use of PPTP involves remote PPTP clients on the untrusted network accessing a local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.
17. A computer-readable storage medium, comprising:	Page 1-7:  Page 10-1: There is a vast wealth of information stored on machines connected

Petitioner Apple Inc. - Exhibit 1002, p. 748

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference
	to the Internet. Page 18-1: The typical use of PPTP involves remote PPTP clients on the untrusted network accessing local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.
a storage area; and	Page 1-7:  Page 10-1: There is a vast wealth of information stored on machines connected to the Internet. Page 18-1: The typical use of PPTP involves remote PPTP clients on the untrusted network accessing local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.
computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:	Preface: In addition to this Administrators Guide, the following resources are available to help you understand and use your Gauntlet Firewall software: Page 1-9: The proxies also check to determine if the request is permitted for the destination. For some services, the proxies can perform the additional step of authenticating the user. This helps verify that users are who they say they are. The proxy then passes the request to the appropriate machine on the other side of the firewall using the standard protocol for that service. Page 18-1: You are concerned about the security of communications on the Internet between your company and your client site. You can use the Point-To-Point Tunneling (PPTP) protocol to provide secure transfer between your site and your client site. The PPTP proxy included with the Gauntlet firewall allows you to

Petitioner Apple Inc. - Exhibit 1002, p. 749

<table>
<tr><th>7,188.180 Claim Elements</th><th>Description for Claimed Elements in the Gauntlet Prior Art Reference</th></tr>
<tr><td></td><td>tunnel PPTP traffic through the firewall. This chapter explains how the PPTP proxy works and how to configure it.
The typical use of PPTP involves remote PPTP clients on the untrusted network accessing a local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.
Page 28-2: For example, consider the situation of a user, John, working at a client site (blaze.clientsite.com) who needs information stored on a machine at work (dimension.yoyodine.com). When John tries to FTP to dimension, which is within the perimeter, he must authenticate at the firewall (fire-out.yoyodyne.com).
The FTP proxy then prompts John for his authentication information (user name and password), which it verifies against the information in the user authentication database. If John provided the proper information, and his account is not disabled, the proxy provides a prompt. John can then connect to dimension on the inside network.
Page 30-5: When nodes on these private networks attempt to communicate with each other (via a VPN) or over a public network (such as the Internet), the reusable (non-routable) IP addresses must be translated to unique, globally routable IP addresses.</td></tr>
<tr><td>receiving a secure domain name;</td><td>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.
Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that policy or proxy, the firewall passes on the request.
Page 5-2: The firewall must perform additional processing steps to convert the address that is in the packet and the hostname that is in the configuration rule to the same format so that it can compare the values, so performance may be slow.
If you deny by host name, the proxy must use DNS to map the source or destination address (in the packet) into a host name.
Page 5-4:
<table>
<tr><th>Parameters</th><th>Enter</th></tr>
<tr><td>IP Address & Mask</td><td>Enter the IP address of the machine to which you want to permit or deny access.

Note: You cannot use the asterisk (*) wildcard in this field.</td></tr>
<tr><td>or Hostname</td><td>Enter a hostname to which you want to permit or deny access, such as www.bigu.edu.</td></tr>
</table></td></tr>
</table>

Petitioner Apple Inc. - Exhibit 1002, p. 750

<table>
<tr><th>7,188,180 Claim Elements</th><th>Description for Claimed Elements in the Gauntlet Prior Art Reference</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>Note: You cannot use the asterisk (*) wildcard in this field.</td></tr>
</table>
Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing.
Page G-1:
<table>
<tr><td>domain name system (DNS)</td><td>The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.</td></tr>
</table>
</td></tr>
<tr><td>sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain name;</td><td>
Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.
Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that policy or proxy, the firewall passes on the request.
Page 5-4:
<table>
<tr><th>Parameters</th><th>Enter</th></tr>
<tr><td>IP Address & Mask</td><td>Enter the IP address of the machine to which you want to permit or deny access.

Note: You cannot use the asterisk (*) wildcard in this field.</td></tr>
<tr><td>or Hostname</td><td>Enter a hostname to which you want to permit or deny access, such as www.bigu.edu.

Note: You cannot use the asterisk (*) wildcard in this field.</td></tr>
</table>
Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing.
Page G-1:
<table>
<tr><td>domain name system (DNS)</td><td>The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.</td></tr>
</table>
</td></tr>
</table>

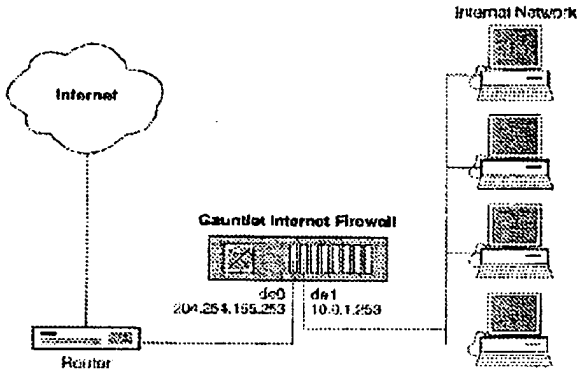
Petitioner Apple Inc. - Exhibit 1002, p. 751

<table>
<tr><th>7,188,180 Claim Elements</th><th>Description for Claimed Elements in the Gauntlet Prior Art Reference</th></tr>
<tr><td>receiving from the domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</td><td>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.
Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that policy or proxy, the firewall passes on the request.
Page 5-4:
<table>
<tr><th>Parameters</th><th>Enter</th></tr>
<tr><td>IP Address & Mask</td><td>Enter the IP address of the machine to which you want to permit or deny access.

Note: You cannot use the asterisk (*) wildcard in this field.</td></tr>
<tr><td>or Hostname</td><td>Enter a hostname to which you want to permit or deny access, such as www.bigu.edu.

Note: You cannot use the asterisk (*) wildcard in this field.</td></tr>
</table>
Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing.
Page G-1:
<table>
<tr><td>domain name system (DNS)</td><td>The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.</td></tr>
</table></td></tr>
</table>

Petitioner Apple Inc. - Exhibit 1002, p. 752

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference
sending an access request message to the secure computer network address using a virtual private network communication link.	Page 1-7:  Page 18-1: You are concerned about the security of communications on the Internet between your company and your client site. You can use the Point-To-Point Tunneling (PPTP) protocol to provide secure transfer between your site and your client site. The PPTP proxy included with the Gauntlet firewall allows you to tunnel PPTP traffic through the firewall. This chapter explains how the PPTP proxy works and how to configure it. The typical use of PPTP involves remote PPTP clients on the untrusted network accessing a local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.
20. The computer-readable medium according to claim 17, wherein the response message contains provisioning information for the virtual private network.	Page 1-8. Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall. Page 5-4:

Petitioner Apple Inc. - Exhibit 1002, p. 753

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference

Parameters	Enter
IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. **Note:** You cannot use the asterisk (*) wildcard in this field.
or Hostname	Enter a hostname to which you want to permit or deny access, such as **www.bigu.edu**. **Note:** You cannot use the asterisk (*) wildcard in this field.

Pages 18-1 - 18-4: You are concerned about the security of communications on the Internet between your company and your client site. You can use the Point-To-Point Tunneling (PPTP) protocol to provide secure transfer between your site and your client site. The PPTP proxy included with the Gauntlet firewall allows you to tunnel PPTP traffic through the firewall. This chapter explains how the PPTP proxy works and how to configure it.

. . . .

Configuring the firewall to allow PPTP traffic involves several steps that must be coordinated. You must configure:

The PPTP proxy to allow TCP Control connections
Policies to allow the PPTP proxy
Packet Screening to allow IP Data connections
Packet Screening to absorb incoming TCP Control connections
Routing on the PPTP client and server machines

. . . .

Configuring the PPTP Proxy

PPTP tunnels are initiated by client machines. Perform the following steps to configure the PPTP proxy to allow connections from all the desired clients.

. . . .

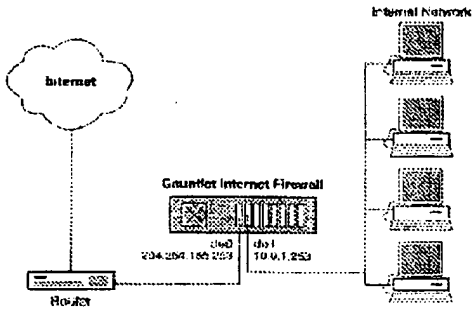
5. Provide information about the hosts that will communicate through the PPTP proxy.

- Enter the IP address and mask or the host name of the machine or network sending PPTP requests. The asterisk wildcard (*) is valid in host names.
- Enter the IP address or host name of the hosts to which the PPTP proxy should connect.
- Enter the port number of the remote host to which the PPTP proxy sends requests. The default port is 1723.
- If desired, enter a description for your rule.

Page G-1:

domain name system (DNS)	The online distributed database system used to map human-readable

Petitioner Apple Inc. - Exhibit 1002, p. 754

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference
	machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.
26. The computer-readable medium according to claim 17, wherein the virtual private network includes the Internet.	Page 1-7:  Page 30-5: When nodes on these private networks attempt to communicate with each other (via a VPN) or over a public network (such as the Internet), the reusable (non-routable) IP addresses must be translated to unique, globally routable IP addresses.
28. The computer readable medium of claim 17, wherein the access request message contains a request for information stored at the secure computer network address.	Page 18-1: You are concerned about the security of communications on the Internet between your company and your client site. You can use the Point-To-Point Tunneling (PPTP) protocol to provide secure transfer between your site and your client site. The PPTP proxy included with the Gauntlet firewall allows you to tunnel PPTP traffic through the firewall. This chapter explains how the PPTP proxy works and how to configure it. The typical use of PPTP involves remote PPTP clients on the untrusted network accessing a local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.
29. The computer-readable medium according to claim 17,	

Petitioner Apple Inc. - Exhibit 1002, p. 755

<table>
<tr><th>7,188,180 Claim Elements</th><th>Description for Claimed Elements in the Gauntlet Prior Art Reference</th></tr>
<tr><td>wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;</td><td>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.
Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that policy or proxy, the firewall passes on the request.
Page 5-2: The firewall must perform additional processing steps to convert the address that is in the packet and the hostname that is in the configuration rule to the same format so that it can compare the values, so performance may be slow.
If you deny by host name, the proxy must use DNS to map the source or destination address (in the packet) into a host name.
Page 5-4:
<table><tr><th>Parameters</th><th>Enter</th></tr><tr><td>IP Address & Mask</td><td>Enter the IP address of the machine to which you want to permit or deny access.

Note: You cannot use the asterisk (*) wildcard in this field.</td></tr><tr><td>or Hostname</td><td>Enter a hostname to which you want to permit or deny access, such as <u>www.bigu.edu</u>.

Note: You cannot use the asterisk (*) wildcard in this field.</td></tr></table>Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing.
Page G-1:
<table><tr><td>domain name system (DNS)</td><td>The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.</td></tr></table></td></tr>
<tr><td>wherein sending the query message comprises sending the query message at the client computer;</td><td>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.
Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the</td></tr>
</table>

Petitioner Apple Inc. - Exhibit 1002, p. 756

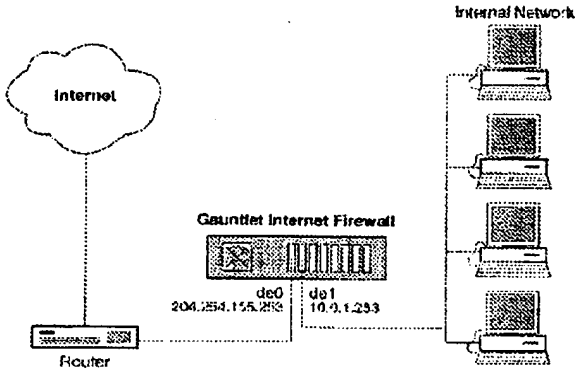
<table>
<tr><th>7,188,180 Claim Elements</th><th>Description for Claimed Elements in the Gauntlet Prior Art Reference</th></tr>
<tr><td></td><td>request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that policy or proxy, the firewall passes on the request.
Page 5-4:
<table><tr><th>Parameters</th><th>Enter</th></tr><tr><td>IP Address & Mask</td><td>Enter the IP address of the machine to which you want to permit or deny access.

Note: You cannot use the asterisk (*) wildcard in this field.</td></tr><tr><td>or Hostname</td><td>Enter a hostname to which you want to permit or deny access, such as www.bigu.edu.

Note: You cannot use the asterisk (*) wildcard in this field.</td></tr></table>Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing.
Page G-1:
<table><tr><td>domain name system (DNS)</td><td>The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.</td></tr></table></td></tr>
<tr><td>wherein receiving the response message comprises receiving the response message at the client computer,</td><td>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.
Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that policy or proxy, the firewall passes on the request
Page 5-4:
<table><tr><th>Parameters</th><th>Enter</th></tr><tr><td>IP Address & Mask</td><td>Enter the IP address of the machine to which you want to permit or deny access.

Note: You cannot use the asterisk (*) wildcard in this field.</td></tr><tr><td>or Hostname</td><td>Enter a hostname to which you want to permit or deny access, such as www.bigu.edu.</td></tr></table></td></tr>
</table>

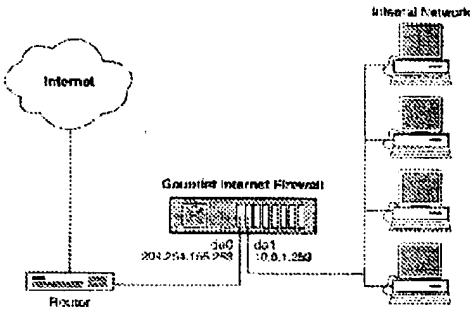
Petitioner Apple Inc. - Exhibit 1002, p. 757

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference
	Note: You cannot use the asterisk (*) wildcard in this field. Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing. Page G-1: domain name system (DNS) — The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.
wherein sending the access request message comprises sending the access request message at the client computer.	Page 1-7:  Page 18-1: You are concerned about the security of communications on the Internet between your company and your client site. You can use the Point-To-Point Tunneling (PPTP) protocol to provide secure transfer between your site and your client site. The PPTP proxy included with the Gauntlet firewall allows you to tunnel PPTP traffic through the firewall. This chapter explains how the PPTP proxy works and how to configure it. The typical use of PPTP involves remote PPTP clients on the untrusted network accessing a local server

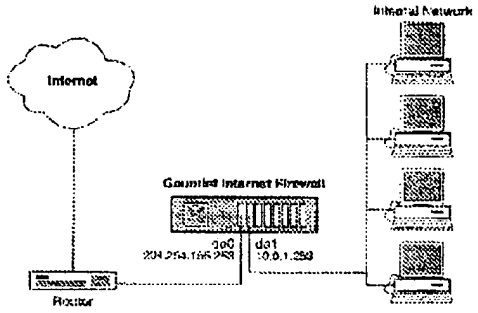
Petitioner Apple Inc. - Exhibit 1002, p. 758

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference
	on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.
30. The computer-readable medium according to claim 17, wherein the method is performed by a software module.	*See* claim 1, which is performed by software at the client computer (e.g., Internet browser, Windows NT, other software the user may use). Page 18-1: The typical use of PPTP involves remote PPTP clients on the untrusted network accessing a local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.
31. The computer-readable medium according to claim 17, wherein the method is performed by a client computer.	*See* claim 1, which is performed by software at the client computer (e.g., Internet browser, Windows NT, other software the user may use). Page 18-1: The typical use of PPTP involves remote PPTP clients on the untrusted network accessing a local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.

Petitioner Apple Inc. - Exhibit 1002, p. 759

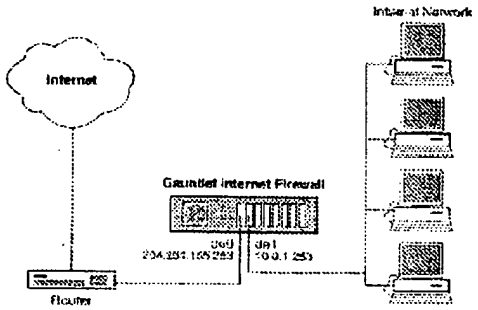
7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference
33. A data processing apparatus, comprising:	Page 1-7:  Page 1-8: Processing packets and requests The firewall follows a standard set of steps for the packets it receives: 1. Receive packet 2. Check source and destination 3. Check request type 4. Call appropriate program 5. Process the request As we examine each step of the process, consider a Yoyodyne employee working at a client site (outside the perimeter) who needs access to her machine at work via TELNET. Page 18-1: The typical use of PPTP involves remote PPTP clients on the untrusted network accessing local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.

Petitioner Apple Inc. - Exhibit 1002, p. 760

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference
a processor, and	Page 1-7:  Page 18-1: The typical use of PPTP involves remote PPTP clients on the untrusted network accessing local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.
memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:	Preface: In addition to this Administrators Guide, the following resources are available to help you understand and use your Gauntlet Firewall software: Page 1-1: The Gauntlet Firewall is a software-based firewall system that provides secure access and internetwork communications between private networks and public networks (such as the Internet), and between subnets of private networks. The firewall offers application-level security services for both incoming and outgoing communications based on existing security practices or an organization's security policies. Page 1-4: The software on the Gauntlet Firewall includes security services for a number of popular applications. Each application generally talks through a different proxy that understands the protocol for that application. Page 1-7:

Petitioner Apple Inc. - Exhibit 1002, p. 761

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference



Page 1-9: The proxies also check to determine if the request is permitted for the destination. For some services, the proxies can perform the additional step of authenticating the user. This helps verify that users are who they say they are. The proxy then passes the request to the appropriate machine on the other side of the firewall using the standard protocol for that service.

Page 7-6:

The following table describes FTP operations.

FTP Operation	Description
CWD/CDUP	Change working directory.
DELE	Delete a file.
LIST/NLIST	List files in a directory.
MKD	Make a directory.
RETR	Retrieve a file.
RMD	Remove a directory.
STOR/STOU	Store or copy a file.
SITE	Access commands supported by site request such as request, unmask, idle, and chmod.

Page 18-1: The typical use of PPTP involves remote PPTP clients on the untrusted network accessing local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.

Petitioner Apple Inc. - Exhibit 1002, p. 762

<table>
<tr><th>7,188,180 Claim Elements</th><th>Description for Claimed Elements in the Gauntlet Prior Art Reference</th></tr>
<tr><td></td><td>Page 28-2: For example, consider the situation of a user, John, working at a client site (blaze.clientsite.com) who needs information stored on a machine at work (dimension.yoyodine.com). When John tries to FTP to dimension, which is within the perimeter, he must authenticate at the firewall (fire-out.yoyodyne.com).
The FTP proxy then prompts John for his authentication information (user name and password), which it verifies against the information in the user authentication database. If John provided the proper information, and his account is not disabled, the proxy provides a prompt. John can then connect to dimension on the inside network.</td></tr>
<tr><td>receiving a secure domain name;</td><td>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.
Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that policy or proxy, the firewall passes on the request.
Page 5-2: The firewall must perform additional processing steps to convert the address that is in the packet and the hostname that is in the configuration rule to the same format so that it can compare the values, so performance may be slow.
If you deny by host name, the proxy must use DNS to map the source or destination address (in the packet) into a host name.
Page 5-4:
<table>
<tr><th>Parameters</th><th>Enter</th></tr>
<tr><td>IP Address & Mask</td><td>Enter the IP address of the machine to which you want to permit or deny access.

Note: You cannot use the asterisk (*) wildcard in this field.</td></tr>
<tr><td>or Hostname</td><td>Enter a hostname to which you want to permit or deny access, such as www.bigu.edu.

Note: You cannot use the asterisk (*) wildcard in this field.</td></tr>
</table>
Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing.
Page G-1:
<table>
<tr><td>domain name system (DNS)</td><td>The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace</td></tr>
</table></td></tr>
</table>

Petitioner Apple Inc. - Exhibit 1002, p. 763

<table>
<tr><th>7,188,180 Claim Elements</th><th>Description for Claimed Elements in the Gauntlet Prior Art Reference</th></tr>
<tr><td></td><td>that allows sites to assign machine names and addresses.</td></tr>
<tr><td>sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;</td><td>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.
Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that policy or proxy, the firewall passes on the request.
Page 5-4:
<table><tr><th>Parameters</th><th>Enter</th></tr><tr><td>IP Address & Mask</td><td>Enter the IP address of the machine to which you want to permit or deny access.

Note: You cannot use the asterisk (*) wildcard in this field.</td></tr><tr><td>or Hostname</td><td>Enter a hostname to which you want to permit or deny access, such as www.bigu.edu.

Note: You cannot use the asterisk (*) wildcard in this field.</td></tr></table>Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing.
Page G-1:
<table><tr><td>domain name system (DNS)</td><td>The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.</td></tr></table></td></tr>
<tr><td>receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and</td><td>Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall.
Page 5-1: If the request is for a site that is denied for that policy and that proxy, the firewall denies the request and logs the attempt. If the request is for a site that is not denied or is explicitly permitted for that policy or proxy, the firewall passes on the request.
Page 5-4:</td></tr>
</table>

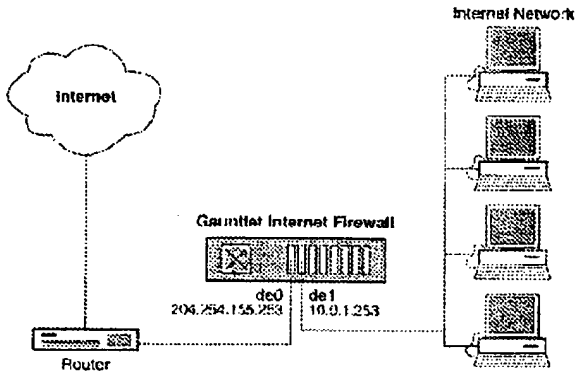
Petitioner Apple Inc. - Exhibit 1002, p. 764

<table>
<tr><th>7,188,180 Claim Elements</th><th>Description for Claimed Elements in the Gauntlet Prior Art Reference</th></tr>
<tr><td></td><td>
<table>
<tr><th>Parameters</th><th>Enter</th></tr>
<tr><td>IP Address & Mask</td><td>Enter the IP address of the machine to which you want to permit or deny access.

Note: You cannot use the asterisk (*) wildcard in this field.</td></tr>
<tr><td>or Hostname</td><td>Enter a hostname to which you want to permit or deny access, such as www.bigu.edu.

Note: You cannot use the asterisk (*) wildcard in this field.</td></tr>
</table>
Page 20-1: A common policy is to have one mail hub for the inside network but to use transparent access for outside networks. The outside networks know (via DNS) they should send all mail for the domains on the inside networks (yoyodyne.com) to the firewall (fire-out.yoyodyne.com) itself for processing.
Page G-1:
<table>
<tr><td>domain name system (DNS)</td><td>The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to assign machine names and addresses.</td></tr>
</table>
</td></tr>
<tr><td>sending an access request message to the secure computer network address using a virtual private network communication link.</td><td>Page 1-7:</td></tr>
</table>

Petitioner Apple Inc. - Exhibit 1002, p. 765

7,188.180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference
	 Page 18-1: You are concerned about the security of communications on the Internet between your company and your client site. You can use the Point-To-Point Tunneling (PPTP) protocol to provide secure transfer between your site and your client site. The PPTP proxy included with the Gauntlet firewall allows you to tunnel PPTP traffic through the firewall. This chapter explains how the PPTP proxy works and how to configure it. The typical use of PPTP involves remote PPTP clients on the untrusted network accessing a local server on the trusted network. For example, traveling employees who have PPTP client software on their laptops can connect to the corporate PPTP server to read mail or access other internal data. You can configure the firewall to allow PPTP traffic between the remote clients and the corporate server.
35. The apparatus of claim 33, wherein the response message contains provisioning information for the virtual private network.	Page 1-8: Routing information on outside hosts and at the ISP directs all requests for the inside network to the firewall. In addition, the domain name system (DNS) on the firewall and other outside DNS servers advertises the outside IP address of the firewall as the only way to connect to anything on the inside network. Hosts on the inside network use routing information to direct all requests for outside networks to the inside address of the firewall. Page 5-4: **Parameters** | **Enter**

Petitioner Apple Inc. - Exhibit 1002, p. 766

7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference

IP Address & Mask	Enter the IP address of the machine to which you want to permit or deny access. **Note:** You cannot use the asterisk (*) wildcard in this field.
or Hostname	Enter a hostname to which you want to permit or deny access, such as **www.bigu.edu**. **Note:** You cannot use the asterisk (*) wildcard in this field.

Pages 18-1 - 18-4: You are concerned about the security of communications on the Internet between your company and your client site. You can use the Point-To-Point Tunneling (PPTP) protocol to provide secure transfer between your site and your client site. The PPTP proxy included with the Gauntlet firewall allows you to tunnel PPTP traffic through the firewall. This chapter explains how the PPTP proxy works and how to configure it.

. . . .

Configuring the firewall to allow PPTP traffic involves several steps that must be coordinated. You must configure:

The PPTP proxy to allow TCP Control connections
Policies to allow the PPTP proxy
Packet Screening to allow IP Data connections
Packet Screening to absorb incoming TCP Control connections
Routing on the PPTP client and server machines

. . . .

Configuring the PPTP Proxy

PPTP tunnels are initiated by client machines. Perform the following steps to configure the PPTP proxy to allow connections from all the desired clients.

. . . .

5. Provide information about the hosts that will communicate through the PPTP proxy.

- Enter the IP address and mask or the host name of the machine or network sending PPTP requests. The asterisk wildcard (*) is valid in host names.
- Enter the IP address or host name of the hosts to which the PPTP proxy should connect.
- Enter the port number of the remote host to which the PPTP proxy sends requests. The default port is 1723.
- If desired, enter a description for your rule.

Page G-1:

domain name system (DNS)	The online distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the Internet implement a hierarchical namespace that allows sites to

Petitioner Apple Inc. - Exhibit 1002, p. 767

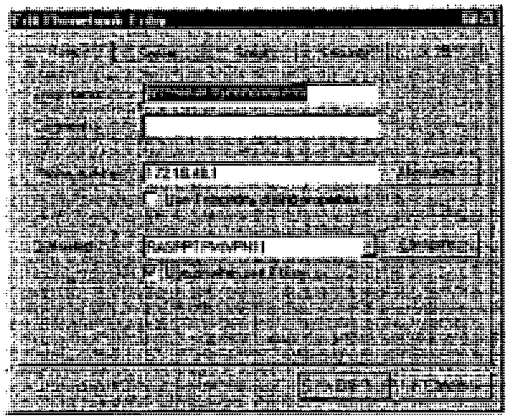
7,188,180 Claim Elements	Description for Claimed Elements in the Gauntlet Prior Art Reference
	assign machine names and addresses.

Petitioner Apple Inc. - Exhibit 1002, p. 768

Appendix G
Citations to Exemplary Description in the Hands On and Installing NT References*

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
1. A method for accessing a secure computer network address, comprising steps of:	Hands On Page 431: Point-to-Point Tunneling Protocol (PPTP) is a technology that supports multiprotocol virtual private networks (VPNs). This support enables you to remotely access your corporate network securely across the Internet." Hands On Page 432: *Security*. PPTP provides security through data encryption. A PPTP connection over the Internet is encrypted and works with the NetBEUI, TCP/IP, and IPX protocols. Data sent by means of a PPTP tunnel consists of encapsulated PPP packets. If Dial-Up Networking is configured to use data encryption, the data sent by means of PPTP is encrypted when sent. Hands On, Page 435: The Point-to-Point Protocol (PPP) was designed as an enhancement to the original SLIP specification. PPP is a set of industry standard framing and authentication protocols that enable RAS clients and servers to interoperate in a multivendor network. Hands On Page 438: Windows NT Server provides for enterprise-wide security using a trusted domain, single-network logon model. This eliminates the need for duplicate user accounts across a multiple-server network. The single-network logon model extends to RAS users. The RAS server uses the same user account database as the computer running Windows NT. This allows easier administration, because clients can log on with the same user accounts that they use at the office. This feature ensures that clients have the same privileges and permissions they ordinarily have while in the office. To connect to a RAS server, clients must have a valid Windows NT user account as well as the RAS dial-in permission. Clients must first be authenticated by RAS before they can log on to Windows NT. Hands On Page 447: **Encryption settings** — Select an authentication level ranging from clear text for down level clients to Microsoft Encrypted Authentication for Windows NT and Windows 95 clients. If **Required Microsoft encrypted authentication** is selected, **Require data encryption** can also be selected. Installing NT at abstract: You can use PPTP to provide secure, on-demand, virtual networks by using dial-up lines, local area networks (LANS), wide area networks (WANS), or the internet and other public, TCP/IP-based networks.
receiving a secure domain name;	Installing NT Pages 20 - 21: 5. Type the IP address of the adapter on the PPTP server that is connected to the internet in the **Phone Number** dialog box. **Note** If your PPTP server has an internet registered DNS name, you could alternatively enter its DNS name in this field.

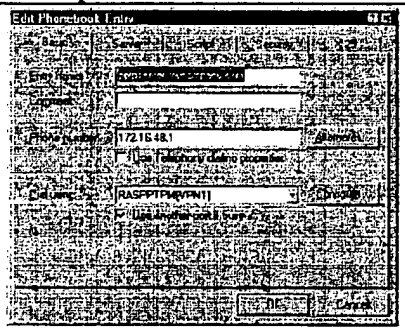
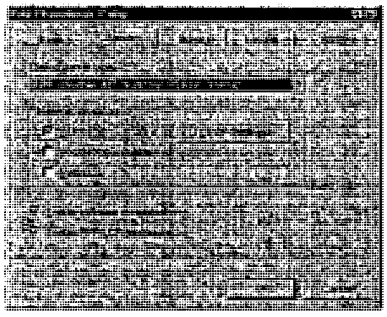
* - The cited passages are an indication of where in the Hands On and Installing NT references, at the very least, the claims find exemplary description. Requestor reserves the right to identify and demonstrate additional description if necessary or desirable.

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
	 *Figure 12 - Example Phonebook entry for PPTP server and a VPN device*
sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;	Hands On Page 401: DNS name servers perform name resolution by interpreting network information to find a specific IP address. The name resolution process is outlined below: 1. A resolver (or client) passes a query to its local name server. 2. If the local name server does not have the data requested in the query, it queries other name servers on behalf of the resolver. 3. When the local name server has the address requested, it returns the information to the resolver. Hands On Page 405: Windows NT Server, Windows NT Workstation, Windows 95, and Windows for Workgroups 3.11 with Microsoft TCP/IP-32 installed all include DNS-resolver functionality. Hands On Page 462: RAS AutoDial maps and maintains network addresses to phonebook entries, allowing them to be automatically dialed when referenced from an application or from the command line. The database can include IP addresses (for example, '127.95.1.4'), Internet host names (for example, 'www.microsoft.com'), or NetBIOS names (for example, 'products1'). Associated with each address in the AutoDial database is a set of one or more entries. Each of these entries specifies a phonebook entry that RAS can dial to connect to the address from a particular TAPI dialing location.
receiving from the secure	Hands On Page 401: DNS name servers perform name resolution by interpreting network information to find a specific

Petitioner Apple Inc. - Exhibit 1002, p. 770

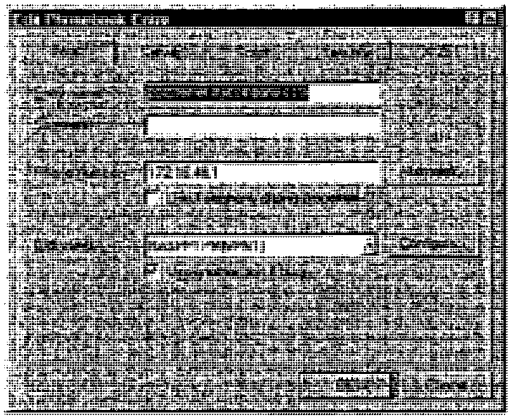
7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
domain name service a response message containing the secure computer network address corresponding to the secure domain name; and	IP address. The name resolution process is outlined below: 1. A resolver (or client) passes a query to its local name server. 2. If the local name server does not have the data requested in the query, it queries other name servers on behalf of the resolver. 3. When the local name server has the address requested, it returns the information to the resolver. Hands On Page 405: Windows NT Server, Windows NT Workstation, Windows 95, and Windows for Workgroups 3.11 with Microsoft TCP/IP-32 installed all include DNS-resolver functionality. Hands On Page 462: RAS AutoDial maps and maintains network addresses to phonebook entries, allowing them to be automatically dialed when referenced from an application or from the command line. The database can include IP addresses (for example, '127.95.1.4'), Internet host names (for example, 'www.microsoft.com'), or NetBIOS names (for example, 'products1'). Associated with each address in the AutoDial database is a set of one or more entries. Each of these entries specifies a phonebook entry that RAS can dial to connect to the address from a particular TAPI dialing location.
sending an access request message to the secure computer network address using a virtual private network communication link.	Hands On Page 431: Point-to-Point Tunneling Protocol (PPTP) is a technology that supports multiprotocol virtual private networks (VPNs). This support enables you to remotely access your corporate network securely across the Internet."
4. The method according to claim 1, wherein the response message contains provisioning information for the virtual private network.	Installing NT at abstract: You can use PPTP to provide secure, on-demand, virtual networks by using dial-up lines, local area networks (LANS), wide area networks (WANS), or the internet and other public, TCP/IP-based networks. Installing NT Page 20: **Creating the Phonebook Entry to Dial a PPTP Server** You must create a phonebook entry to connect to your PPTP server by using a VPN device. . . . . 5: Type the IP address of the adapter on the PPTP server that is connected to the Internet in the Phone Number dialog box. Installing NT Page 21: Note If your PPTP server has an Internet registered DNS name, you could alternatively enter it's DNS name in this field. . . . . *To verify or edit your phonebook entry for the PPTP server* 1. Click More in Dial-Up Networking, and then click Edit entry and modem properties to verify that your PPTP server phonebook entry is correctly configured. The Edit Phonebook Entry dialog box will appear as illustrated in the following figure.

Petitioner Apple Inc. - Exhibit 1002, p. 771

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
	 Figure 12 - Example Phonebook entry for PPTP server and a VPN device Installing NT Page 22:  Figure 13 - Verifying the Dial-Up Server configuration on the PPTP client . . . . Note If you are configuring the VPN device on an ISP server running Windows NT Server version 4.0 that is configured with

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
	multiple VPN devices, repeat this procedure for each VPN device. Installing NT Page 23: A PPTP-enabled client must have two phonebook entries (as described in the previous section) to connect to a PPTP server. . . . . After successful connection, all traffic through your modem is routed by the ISP over the Internet to your PPTP server, which routes the traffic to the correct computer. Installing NT Page 24: You do not need to make a second dial-up call because the ISP server configured as a PPTP client, makes the connection to the PPTP server for the PPP client.
10. The method according to claim 1, wherein the virtual private network includes the Internet.	Hands On Page 431: Point-to-Point Tunneling Protocol (PPTP) is a technology that supports multiprotocol virtual private networks (VPNs). This support enables you to remotely access your corporate network securely across the Internet."
12. The method of claim 1, wherein the access request message contains a request for information stored at the secure computer network address.	Hands On Page 431: Point-to-Point Tunneling Protocol (PPTP) is a technology that supports multiprotocol virtual private networks (VPNs). This support enables you to remotely access your corporate network securely across the Internet."
13. The method of claim 1,	
wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;	Installing NT Pages 20 - 21: 5. Type the IP address of the adapter on the PPTP server that is connected to the internet in the **Phone Number** dialog box. **Note** If your PPTP server has an internet registered DNS name, you could alternatively enter its DNS name in this field.

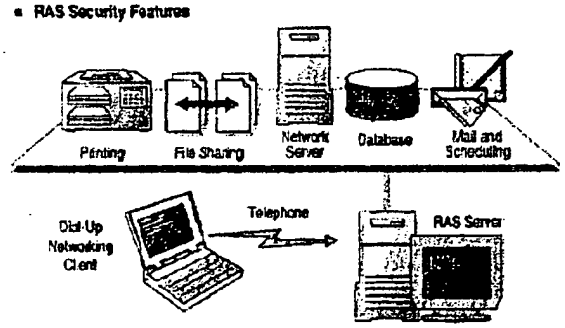
Petitioner Apple Inc. - Exhibit 1002, p. 773

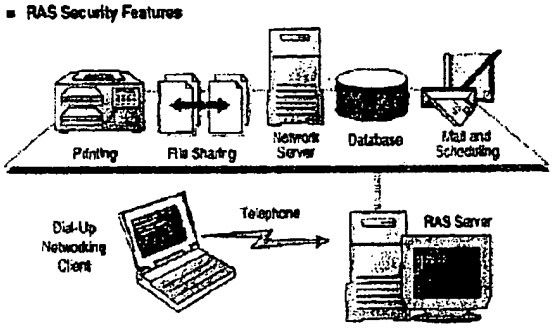
7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
	 *Figure 12 - Example Phonebook entry for PPTP server and a VPN device*
wherein sending the query message comprises sending the query message at the client computer;	Hands On Page 401: DNS name servers perform name resolution by interpreting network information to find a specific IP address. The name resolution process is outlined below: 4. A resolver (or client) passes a query to its local name server. 5. If the local name server does not have the data requested in the query, it queries other name servers on behalf of the resolver. 6. When the local name server has the address requested, it returns the information to the resolver. Hands On Page 405: Windows NT Server, Windows NT Workstation, Windows 95, and Windows for Workgroups 3.11 with Microsoft TCP/IP-32 installed all include DNS-resolver functionality. Hands On Page 462: RAS AutoDial maps and maintains network addresses to phonebook entries, allowing them to be automatically dialed when referenced from an application or from the command line. The database can include IP addresses (for example, '127.95.1.4'), Internet host names (for example, 'www.microsoft.com'), or NetBIOS names (for example, 'products1'). Associated with each address in the AutoDial database is a set of one or more entries. Each of these entries specifies a phonebook entry that RAS can dial to connect to the address from a particular TAPI dialing location.

Petitioner Apple Inc. - Exhibit 1002, p. 774

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
wherein receiving the response message comprises receiving the response message at the client computer,	Hands On Page 401: DNS name servers perform name resolution by interpreting network information to find a specific IP address. The name resolution process is outlined below: 4. A resolver (or client) passes a query to its local name server. 5. If the local name server does not have the data requested in the query, it queries other name servers on behalf of the resolver. 6. When the local name server has the address requested, it returns the information to the resolver. Hands On Page 405: Windows NT Server, Windows NT Workstation, Windows 95, and Windows for Workgroups 3.11 with Microsoft TCP/IP-32 installed all include DNS-resolver functionality. Hands On Page 462: RAS AutoDial maps and maintains network addresses to phonebook entries, allowing them to be automatically dialed when referenced from an application or from the command line. The database can include IP addresses (for example, '127.95.1.4'), Internet host names (for example, 'www.microsoft.com'), or NetBIOS names (for example, 'products1'). Associated with each address in the AutoDial database is a set of one or more entries. Each of these entries specifies a phonebook entry that RAS can dial to connect to the address from a particular TAPI dialing location.
wherein sending the access request message comprises sending the access request message at the client computer.	Hands On Page 431: Point-to-Point Tunneling Protocol (PPTP) is a technology that supports multiprotocol virtual private networks (VPNs). This support enables you to remotely access your corporate network securely across the Internet."
14. The method of claim 1, performed by a software module.	*See* claim 1, which is performed by Windows NT 4.0.
15. The method of claim 1, performed by a client computer.	*See* claim 1, which is performed by Windows NT 4.0 installed and configured at the client computer.
17. A computer-readable storage medium, comprising:	Hands On Page 428:

Petitioner Apple Inc. - Exhibit 1002, p. 775

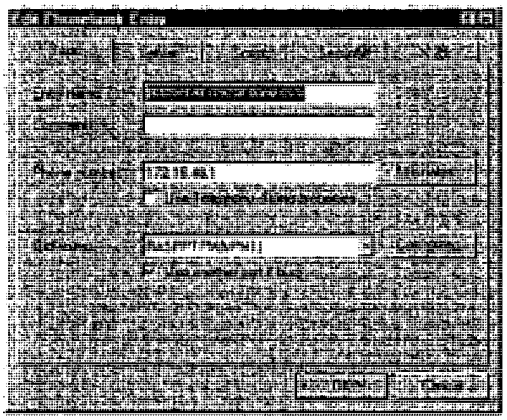
7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
	The following illustration lists some of the principal features of RAS and illustrates the resources that are made available to the Dial-Up Networking client. • WAN Connectivity • Remote Access Protocols • Gateways and Routers • Point-to-Point Tunneling Protocol (PPTP) • RAS Security Features 

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
a storage area; and	Hands On Page 428: The following illustration lists some of the principal features of RAS and illustrates the resources that are made available to the Dial-Up Networking client. ▪ WAN Connectivity ▪ Remote Access Protocols ▪ Gateways and Routers ▪ Point-to-Point Tunneling Protocol (PPTP) ▪ RAS Security Features 
computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:	Hands On Page 431: Point-to-Point Tunneling Protocol (PPTP) is a technology that supports multiprotocol virtual private networks (VPNs). This support enables you to remotely access your corporate network securely across the Internet." Hands On Page 432: *Security*. PPTP provides security through data encryption. A PPTP connection over the Internet is encrypted and works with the NetBEUI, TCP/IP, and IPX protocols. Data sent by means of a PPTP tunnel consists of encapsulated PPP packets. If Dial-Up Networking is configured to use data encryption, the data sent by means of PPTP is encrypted when sent. Hands On Page 435: The Point-to-Point Protocol (PPP) was designed as an enhancement to the original SLIP specification. PPP is a set of industry standard framing and authentication protocols that enable RAS clients and servers to interoperate in a multivendor network.

Petitioner Apple Inc. - Exhibit 1002, p. 777

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
	Hands On Page 438: Windows NT Server provides for enterprise-wide security using a trusted domain, single-network logon model. This eliminates the need for duplicate user accounts across a multiple-server network. The single-network logon model extends to RAS users. The RAS server uses the same user account database as the computer running Windows NT. This allows easier administration, because clients can log on with the same user accounts that they use at the office. This feature ensures that clients have the same privileges and permissions they ordinarily have while in the office. To connect to a RAS server, clients must have a valid Windows NT user account as well as the RAS dial-in permission. Clients must first be authenticated by RAS before they can log on to Windows NT. Hands On Page 447: **Encryption settings** — Select an authentication level ranging from clear text for down level clients to Microsoft Encrypted Authentication for Windows NT and Windows 95 clients. If **Required Microsoft encrypted authentication** is selected, **Require data encryption** can also be selected. Installing NT at abstract: You can use PPTP to provide secure, on-demand, virtual networks by using dial-up lines, local area networks (LANS), wide area networks (WANS), or the internet and other public, TCP/IP-based networks.
receiving a secure domain name;	Installing NT Pages 20 - 21: 5. Type the IP address of the adapter on the PPTP server that is connected to the internet in the **Phone Number** dialog box. **Note** If your PPTP server has an internet registered DNS name, you could alternatively enter its DNS name in this field.

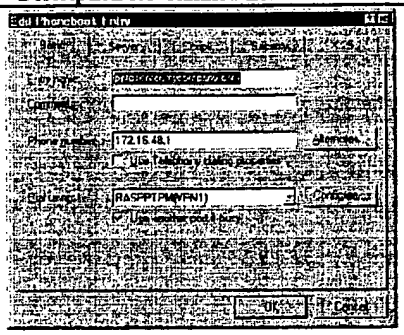
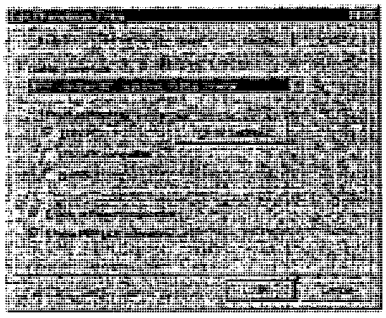
Petitioner Apple Inc. - Exhibit 1002, p. 778

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
	 *Figure 12 - Example Phonebook entry for PPTP server and a VPN device*
sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain name;	Hands On Page 401: DNS name servers perform name resolution by interpreting network information to find a specific IP address. The name resolution process is outlined below: 7. A resolver (or client) passes a query to its local name server. 8. If the local name server does not have the data requested in the query, it queries other name servers on behalf of the resolver. 9. When the local name server has the address requested, it returns the information to the resolver. Hands On Page 405: Windows NT Server, Windows NT Workstation, Windows 95, and Windows for Workgroups 3.11 with Microsoft TCP/IP-32 installed all include DNS-resolver functionality. Hands On Page 462: RAS AutoDial maps and maintains network addresses to phonebook entries, allowing them to be automatically dialed when referenced from an application or from the command line. The database can include IP addresses (for example, '127.95.1.4'), Internet host names (for example, 'www.microsoft.com'), or NetBIOS names (for example, 'products1'). Associated with each address in the AutoDial database is a set of one or more entries. Each of these entries specifies a phonebook entry that RAS can dial to connect to the address from a particular TAPI dialing location.

Petitioner Apple Inc. - Exhibit 1002, p. 779

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
receiving from the domain name service a response message containing the secure computer network address corresponding to the secure domain name; and	Hands On Page 401: DNS name servers perform name resolution by interpreting network information to find a specific IP address. The name resolution process is outlined below: 7. A resolver (or client) passes a query to its local name server. 8. If the local name server does not have the data requested in the query, it queries other name servers on behalf of the resolver. 9. When the local name server has the address requested, it returns the information to the resolver. Hands On Page 405: Windows NT Server, Windows NT Workstation, Windows 95, and Windows for Workgroups 3.11 with Microsoft TCP/IP-32 installed all include DNS-resolver functionality. Hands On Page 462: RAS AutoDial maps and maintains network addresses to phonebook entries, allowing them to be automatically dialed when referenced from an application or from the command line. The database can include IP addresses (for example, '127.95.1.4'), Internet host names (for example, 'www.microsoft.com'), or NetBIOS names (for example, 'products1'). Associated with each address in the AutoDial database is a set of one or more entries. Each of these entries specifies a phonebook entry that RAS can dial to connect to the address from a particular TAPI dialing location.
sending an access request message to the secure computer network address using a virtual private network communication link.	Hands On Page 431: Point-to-Point Tunneling Protocol (PPTP) is a technology that supports multiprotocol virtual private networks (VPNs). This support enables you to remotely access your corporate network securely across the Internet."
20. The computer-readable medium according to claim 17, wherein the response message contains provisioning information for the virtual private network.	Installing NT at abstract: You can use PPTP to provide secure, on-demand, virtual networks by using dial-up lines, local area networks (LANS), wide area networks (WANS), or the internet and other public, TCP/IP-based networks. Installing NT Page 20: **Creating the Phonebook Entry to Dial a PPTP Server** You must create a phonebook entry to connect to your PPTP server by using a VPN device. . . . . 5: Type the IP address of the adapter on the PPTP server that is connected to the Internet in the Phone Number dialog box. Installing NT Page 21: Note If your PPTP server has an Internet registered DNS name, you could alternatively enter it's DNS name in this field. . . . . *To verify or edit your phonebook entry for the PPTP server* 1. Click More in Dial-Up Networking, and then click Edit entry and modem properties to verify that your PPTP server phonebook entry is correctly configured. The Edit Phonebook Entry dialog box will appear as illustrated in the following figure.

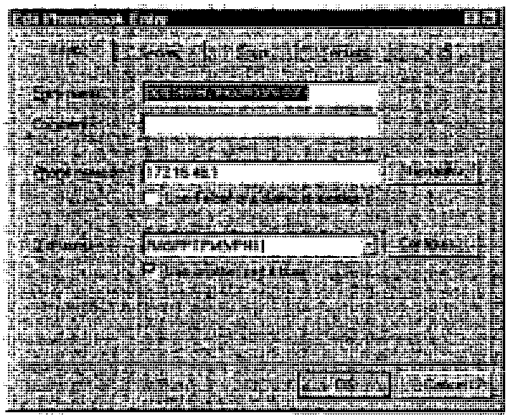
Petitioner Apple Inc. - Exhibit 1002, p. 780

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
	 Figure 12 - Example Phonebook entry for PPTP server and a VPN device Installing NT Page 22:  Figure 13 - Verifying the Dial-Up Server configuration on the PPTP client . . . . Note If you are configuring the VPN device on an ISP server running Windows NT Server version 4.0 that is configured with

Petitioner Apple Inc. - Exhibit 1002, p. 781

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
	multiple VPN devices, repeat this procedure for each VPN device. Installing NT Page 23: A PPTP-enabled client must have two phonebook entries (as described in the previous section) to connect to a PPTP server. . . . . After successful connection, all traffic through your modem is routed by the ISP over the Internet to your PPTP server, which routes the traffic to the correct computer. Installing NT Page 24: You do not need to make a second dial-up call because the ISP server configured as a PPTP client, makes the connection to the PPTP server for the PPP client.
26. The computer-readable medium according to claim 17, wherein the virtual private network includes the Internet.	Hands On Page 431: Point-to-Point Tunneling Protocol (PPTP) is a technology that supports multiprotocol virtual private networks (VPNs). This support enables you to remotely access your corporate network securely across the Internet."
28. The computer readable medium of claim 17, wherein the access request message contains a request for information stored at the secure computer network address.	Hands On Page 431: Point-to-Point Tunneling Protocol (PPTP) is a technology that supports multiprotocol virtual private networks (VPNs). This support enables you to remotely access your corporate network securely across the Internet."
29. The computer-readable medium according to claim 17,	
wherein receiving the secure domain name comprises receiving the secure domain name at a client computer from a user;	Installing NT Pages 20 - 21: 5. Type the IP address of the adapter on the PPTP server that is connected to the internet in the **Phone Number** dialog box. **Note** If your PPTP server has an internet registered DNS name, you could alternatively enter its DNS name in this field.

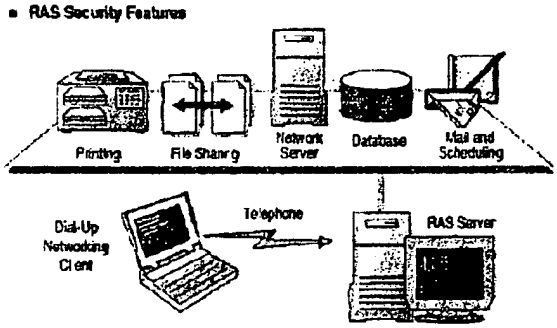
Petitioner Apple Inc. - Exhibit 1002, p. 782

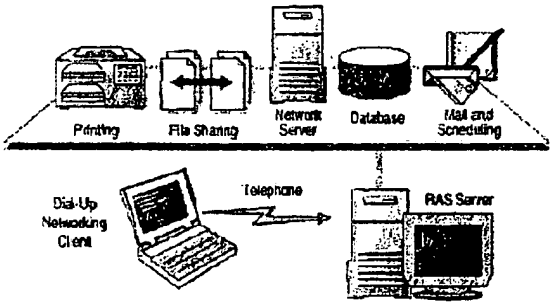
7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
	 Figure 12 - Example Phonebook entry for PPTP server and a VPN device
wherein sending the query message comprises sending the query message at the client computer;	Hands On Page 401: DNS name servers perform name resolution by interpreting network information to find a specific IP address. The name resolution process is outlined below: 10. A resolver (or client) passes a query to its local name server. 11. If the local name server does not have the data requested in the query, it queries other name servers on behalf of the resolver. 12. When the local name server has the address requested, it returns the information to the resolver. Hands On Page 405: Windows NT Server, Windows NT Workstation, Windows 95, and Windows for Workgroups 3.11 with Microsoft TCP/IP-32 installed all include DNS-resolver functionality. Hands On Page 462: RAS AutoDial maps and maintains network addresses to phonebook entries, allowing them to be automatically dialed when referenced from an application or from the command line. The database can include IP addresses (for example, '127.95.1.1'), Internet host names (for example, 'www.microsoft.com'), or NetBIOS names (for example, 'product1'). Associated with each address in the AutoDial database is a set of one or more entries. Each of these entries specifies a phonebook entry that RAS can dial to connect to the address from a particular TAPI dialing location.

Petitioner Apple Inc. - Exhibit 1002, p. 783

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
wherein receiving the response message comprises receiving the response message at the client computer,	Hands On Page 401: DNS name servers perform name resolution by interpreting network information to find a specific IP address. The name resolution process is outlined below: 10. A resolver (or client) passes a query to its local name server. 11. If the local name server does not have the data requested in the query, it queries other name servers on behalf of the resolver. 12. When the local name server has the address requested, it returns the information to the resolver. Hands On Page 405: Windows NT Server, Windows NT Workstation, Windows 95, and Windows for Workgroups 3.11 with Microsoft TCP/IP-32 installed all include DNS-resolver functionality. Hands On Page 462: RAS AutoDial maps and maintains network addresses to phonebook entries, allowing them to be automatically dialed when referenced from an application or from the command line. The database can include IP addresses (for example, '127.95.1.4'), Internet host names (for example, 'www.microsoft.com'), or NetBIOS names (for example, 'products1'). Associated with each address in the AutoDial database is a set of one or more entries. Each of these entries specifies a phonebook entry that RAS can dial to connect to the address from a particular TAPI dialing location.
wherein sending the access request message comprises sending the access request message at the client computer.	Hands On Page 431: Point-to-Point Tunneling Protocol (PPTP) is a technology that supports multiprotocol virtual private networks (VPNs). This support enables you to remotely access your corporate network securely across the Internet."
30. The computer-readable medium according to claim 17, wherein the method is performed by a software module.	*See* claim 1, which is performed by Windows NT 4.0.
31. The computer-readable medium according to claim 17, wherein the method is performed by a client computer.	*See* claim 1, which is performed by Windows NT 4.0 installed and configured at the client computer.

Petitioner Apple Inc. - Exhibit 1002, p. 784

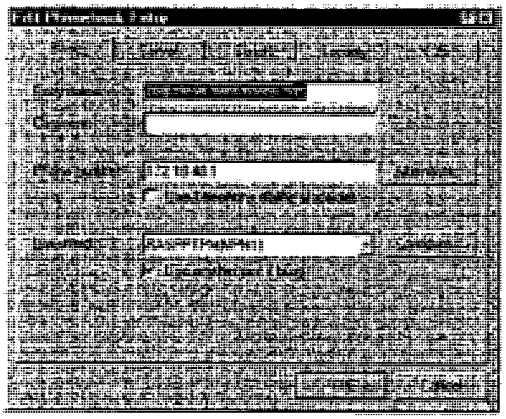
7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
33. A data processing apparatus, comprising:	Hands On Page 428: The following illustration lists some of the principal features of RAS and illustrates the resources that are made available to the Dial-Up Networking client. ▪ WAN Connectivity ▪ Remote Access Protocols ▪ Gateways and Routers ▪ Point-to-Point Tunneling Protocol (PPTP) ▪ RAS Security Features 

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
a processor, and	Hands On Page 428: The following illustration lists some of the principal features of RAS and illustrates the resources that are made available to the Dial-Up Networking client. ▪ WAN Connectivity ▪ Remote Access Protocols ▪ Gateways and Routers ▪ Point-to-Point Tunneling Protocol (PPTP) ▪ RAS Security Features 

Petitioner Apple Inc. - Exhibit 1002, p. 786

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:	Hands On Page 431: Point-to-Point Tunneling Protocol (PPTP) is a technology that supports multiprotocol virtual private networks (VPNs). This support enables you to remotely access your corporate network securely across the Internet." Hands On Page 432: *Security*. PPTP provides security through data encryption. A PPTP connection over the Internet is encrypted and works with the NetBEUI, TCP/IP, and IPX protocols. Data sent by means of a PPTP tunnel consists of encapsulated PPP packets. If Dial-Up Networking is configured to use data encryption, the data sent by means of PPTP is encrypted when sent. Hands On Page 435: The Point-to-Point Protocol (PPP) was designed as an enhancement to the original SLIP specification. PPP is a set of industry standard framing and authentication protocols that enable RAS clients and servers to interoperate in a multivendor network. Hands On Page 438: Windows NT Server provides for enterprise-wide security using a trusted domain, single-network logon model. This eliminates the need for duplicate user accounts across a multiple-server network. The single-network logon model extends to RAS users. The RAS server uses the same user account database as the computer running Windows NT. This allows easier administration, because clients can log on with the same user accounts that they use at the office. This feature ensures that clients have the same privileges and permissions they ordinarily have while in the office. To connect to a RAS server, clients must have a valid Windows NT user account as well as the RAS dial-in permission. Clients must first be authenticated by RAS before they can log on to Windows NT. Hands On Page 447: **Encryption settings** — Select an authentication level ranging from clear text for down level clients to Microsoft Encrypted Authentication for Windows NT and Windows 95 clients. If **Required Microsoft encrypted authentication** is selected, **Require data encryption** can also be selected. Installing NT at abstract: You can use PPTP to provide secure, on-demand, virtual networks by using dial-up lines, local area networks (LANS), wide area networks (WANS), or the internet and other public, TCP/IP-based networks.
receiving a secure domain name;	Installing NT Pages 20 - 21: 5. Type the IP address of the adapter on the PPTP server that is connected to the internet in the **Phone Number** dialog box. **Note** If your PPTP server has an internet registered DNS name, you could alternatively enter its DNS name in this field.

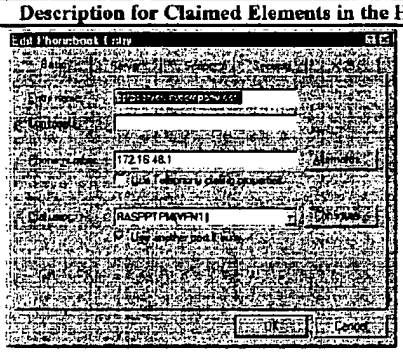
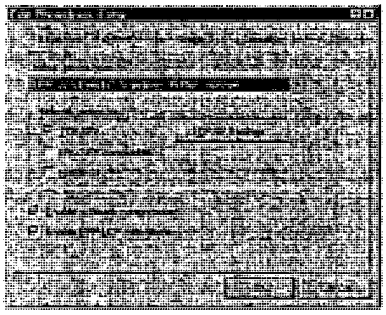
Petitioner Apple Inc. - Exhibit 1002, p. 787

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
	 *Figure 12 - Example Phonebook entry for PPTP server and a VPN device* Installing NT at abstract: You can use PPTP to provide secure, on-demand, virtual networks by using dial-up lines, local area networks (LANS), wide area networks (WANS), or the internet and other public, TCP/IP-based networks.
sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;	Hands On Page 401: DNS name servers perform name resolution by interpreting network information to find a specific IP address. The name resolution process is outlined below: 13. A resolver (or client) passes a query to its local name server. 14. If the local name server does not have the data requested in the query, it queries other name servers on behalf of the resolver. 15. When the local name server has the address requested, it returns the information to the resolver. Hands On Page 405: Windows NT Server, Windows NT Workstation, Windows 95, and Windows for Workgroups 3.11 with Microsoft TCP/IP-32 installed all include DNS-resolver functionality. Hands On Page 462: RAS AutoDial maps and maintains network addresses to phonebook entries, allowing them to be automatically dialed when referenced from an application or from the command line. The database can include IP addresses (for example, '127.95.1.4'), Internet host names (for example, 'www.microsoft.com'), or NetBIOS names (for example, 'products1'). Associated with each address in the AutoDial database is a set of one or more entries. Each of these entries specifies a phonebook entry that RAS can dial to connect to the address from a particular TAPI dialing location.

Petitioner Apple Inc. - Exhibit 1002, p. 788

7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and	Hands On Page 401: DNS name servers perform name resolution by interpreting network information to find a specific IP address. The name resolution process is outlined below: 13. A resolver (or client) passes a query to its local name server. 14. If the local name server does not have the data requested in the query, it queries other name servers on behalf of the resolver. 15. When the local name server has the address requested, it returns the information to the resolver. Hands On Page 405: Windows NT Server, Windows NT Workstation, Windows 95, and Windows for Workgroups 3.11 with Microsoft TCP/IP-32 installed all include DNS-resolver functionality. Hands On Page 462: RAS AutoDial maps and maintains network addresses to phonebook entries, allowing them to be automatically dialed when referenced from an application or from the command line. The database can include IP addresses (for example, '127.95.1.4'), Internet host names (for example, 'www.microsoft.com'), or NetBIOS names (for example, 'products1'). Associated with each address in the AutoDial database is a set of one or more entries. Each of these entries specifies a phonebook entry that RAS can dial to connect to the address from a particular TAPI dialing location.
sending an access request message to the secure computer network address using a virtual private network communication link.	Hands On Page 431: Point-to-Point Tunneling Protocol (PPTP) is a technology that supports multiprotocol virtual private networks (VPNs). This support enables you to remotely access your corporate network securely across the Internet."
35. The apparatus of claim 33, wherein the response message contains provisioning information for the virtual private network.	Installing NT at abstract: You can use PPTP to provide secure, on-demand, virtual networks by using dial-up lines, local area networks (LANS), wide area networks (WANS), or the internet and other public, TCP/IP-based networks. Installing NT Page 20: **Creating the Phonebook Entry to Dial a PPTP Server** You must create a phonebook entry to connect to your PPTP server by using a VPN device. . . . . 5: Type the IP address of the adapter on the PPTP server that is connected to the Internet in the Phone Number dialog box. Installing NT Page 21: Note If your PPTP server has an Internet registered DNS name, you could alternatively enter it's DNS name in this field. . . . . *To verify or edit your phonebook entry for the PPTP server* 1. Click More in Dial-Up Networking, and then click Edit entry and modem properties to verify that your PPTP server phonebook entry is correctly configured. The Edit Phonebook Entry dialog box will appear as illustrated in the following figure.

Petitioner Apple Inc. - Exhibit 1002, p. 789

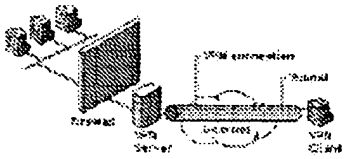
7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
	 Figure 12 - Example Phonebook entry for PPTP server and a VPN device Installing NT Page 22:  Figure 13 - Verifying the Dial-Up Server configuration on the PPTP client . . . . Note If you are configuring the VPN device on an ISP server running Windows NT Server version 4.0 that is configured with

Petitioner Apple Inc. - Exhibit 1002, p. 790

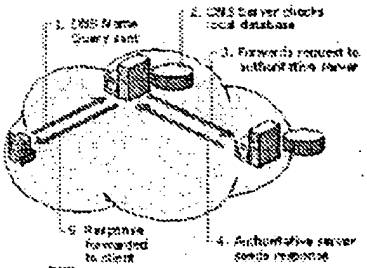
7,188,180 Claim Elements	Description for Claimed Elements in the Hands On and Installing NT Prior Art References
	multiple VPN devices, repeat this procedure for each VPN device. Installing NT Page 23: A PPTP-enabled client must have two phonebook entries (as described in the previous section) to connect to a PPTP server. . . . . After successful connection, all traffic through your modem is routed by the ISP over the Internet to your PPTP server, which routes the traffic to the correct computer. Installing NT Page 24: You do not need to make a second dial-up call because the ISP server configured as a PPTP client, makes the connection to the PPTP server for the PPP client.

Petitioner Apple Inc. - Exhibit 1002, p. 791

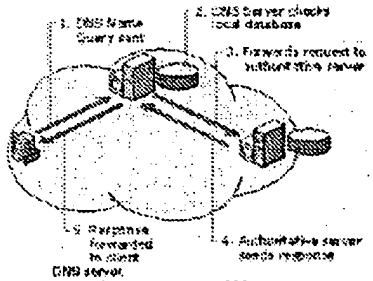
Appendix H
Citations to Exemplary Description in the Microsoft VPN*

7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
1. A method for accessing a secure computer network address, comprising steps of:	Microsoft VPN, Page 11: Microsoft® Windows® NT 4.0 includes support for virtual private networking technology, which leverages the IP connectivity of the Internet to connect remote clients and remote offices. As a network professional, you should understand the important uses of virtual private networking for your organization and the underlying technologies that make it work: the Point-to-Point Tunneling Protocol (PPTP), virtual private networks and security, virtual private networks and routing and translation, virtual private networks and firewalls, and the troubleshooting of virtual private network connections. You should already be familiar with TCP/IP, IP routing, and the Windows NT 4.0 remote access server. Microsoft VPN, Page 13: For the VPN connection to be established, the VPN server authenticates the VPN client attempting the connection and verifies that the VPN client has the appropriate permissions. If mutual authentication is being used, the VPN client also authenticates the VPN server, providing protection against masquerading VPN servers. Microsoft VPN, Page 34:  Figure 13: VPN Server on the Internet in Front of the Firewall
receiving a secure domain name;	Microsoft VPN, Page 32: Create a demand-dial interface for the router-to-router VPN connection with the corporate office router configured for a PPTP device, the IP address or host name of the corporate office VPN server's interface on the Internet, and a user name and password that can be verified by the VPN server. The user name must match the name of a demand-dial interface on the corporate office VPN server.
sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;	Microsoft VPN, Page 66:

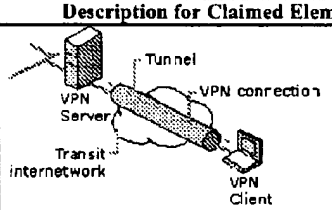
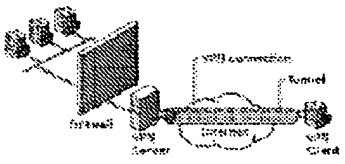
* - The cited passages are an indication of where in the Microsoft VPN reference, at the very least, the claims find exemplary description. Requestor reserves the right to identify and demonstrate additional description if necessary or desirable.

7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	The following process outlines what happens when the DNS resolver component on a host sends a DNS query to a DNS server. This example is shown in Figure 12 and is deliberately simplified to gain a basic understanding of the DNS resolution process. 1. The DNS resolver component formats a DNS Name Query containing the FQDN and sends it to the configured DNS server.  2. The DNS server checks the FQDN in the DNS Name Query against locally stored address records. If a record is found, the IP address corresponding to the requested FQDN is sent back to the client. 3. If the FQDN is not found, the DNS server forwards the request to a DNS server that is authoritative for the FQDN. 4. The authoritative DNS server returns the reply, containing the resolved IP address, back to the original DNS server. 5. The original DNS server sends the IP address mapping information to the client.
receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and	Microsoft VPN, Page 66:

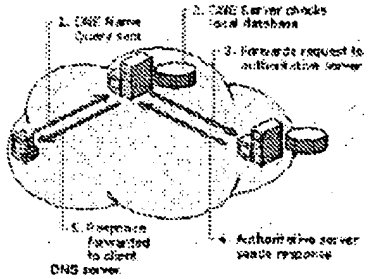
Petitioner Apple Inc. - Exhibit 1002, p. 793

7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	The following process outlines what happens when the DNS resolver component on a host sends a DNS query to a DNS server. This example is shown in Figure 12 and is deliberately simplified to gain a basic understanding of the DNS resolution process. 1. The DNS resolver component formats a DNS Name Query containing the FQDN and sends it to the configured DNS server.  2. The DNS server checks the FQDN in the DNS Name Query against locally stored address records. If a record is found, the IP address corresponding to the requested FQDN is sent back to the client. 3. If the FQDN is not found, the DNS server forwards the request to a DNS server that is authoritative for the FQDN. 4. The authoritative DNS server returns the reply, containing the resolved IP address, back to the original DNS server. 5. The original DNS server sends the IP address mapping information to the client.
sending an access request message to the secure computer network address using a virtual private network communication link.	Microsoft VPN Page 11: VPN connections allow users working at home or on the road to obtain remote access connection to an organization server using the infrastructure provided by public internetwork such as the Internet. . . . A VPN enables you to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link. Microsoft VPN Page 12:

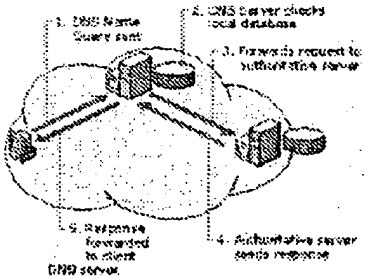
Petitioner Apple Inc. - Exhibit 1002, p. 794

7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	
10. The method according to claim 1, wherein the virtual private network includes the Internet.	Microsoft VPN, Page 34: 
12. The method of claim 1, wherein the access request message contains a request for information stored at the secure computer network address.	Microsoft VPN, Page 11: A VPN enables you to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link. . . . . VPN connections allow users working at home or on the road to obtain remote access connection to an organization server using the infrastructure provided by public internetwork such as the Internet.
13. The method of claim 1,	
wherein receiving the secure domain name comprises receiving the secure domain name at a client computer	Microsoft VPN, Page 32: Create a demand-dial interface for the router-to-router VPN connection with the corporate office router configured for a PPTP device. the IP address or host name of the corporate office VPN server's interface on the Internet, and a user name and password that can be verified by the VPN server. The user

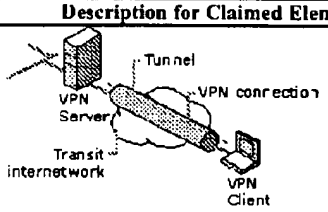
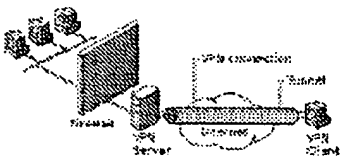
Petitioner Apple Inc. - Exhibit 1002, p. 795

7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
from a user;	name must match the name of a demand-dial interface on the corporate office VPN server.
wherein sending the query message comprises sending the query message at the client computer;	Microsoft VPN, Page 66: The following process outlines what happens when the DNS resolver component on a host sends a DNS query to a DNS server. This example is shown in Figure 12 and is deliberately simplified to gain a basic understanding of the DNS resolution process. 1. The DNS resolver component formats a DNS Name Query containing the FQDN and sends it to the configured DNS server.  2. The DNS server checks the FQDN in the DNS Name Query against locally stored Address records. If a record is found, the IP address corresponding to the requested FQDN is sent back to the client. 3. If the FQDN is not found, the DNS server forwards the request to a DNS server that is authoritative for the FQDN. 4. The authoritative DNS server returns the reply, containing the resolved IP address, back to the original DNS server. 5. The original DNS server sends the IP address mapping information to the client.
wherein receiving the response message comprises receiving the response message at the client computer,	Microsoft VPN, Page 66:

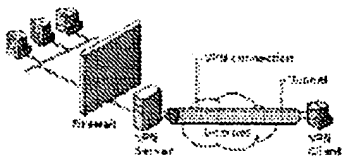
Petitioner Apple Inc. - Exhibit 1002, p. 796

7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	The following process outlines what happens when the DNS resolver component on a host sends a DNS query to a DNS server. This example is shown in Figure 12 and is deliberately simplified to gain a basic understanding of the DNS resolution process. 1. The DNS resolver component formats a DNS Name Query containing the FQDN and sends it to the configured DNS server.  2. The DNS server checks the FQDN in the DNS Name Query against locally stored address records. If a record is found, the IP address corresponding to the requested FQDN is sent back to the client. 3. If the FQDN is not found, the DNS server forwards the request to a DNS server that is authoritative for the FQDN. 4. The authoritative DNS server returns the reply, containing the resolved IP address, back to the original DNS server. 5. The original DNS server sends the IP address mapping information to the client.
wherein sending the access request message comprises sending the access request message at the client computer.	Microsoft VPN Page 11: VPN connections allow users working at home or on the road to obtain remote access connection to an organization server using the infrastructure provided by public internetwork such as the Internet. . . . A VPN enables you to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link. Microsoft VPN Page 12:

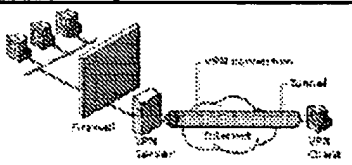
Petitioner Apple Inc. - Exhibit 1002, p. 797

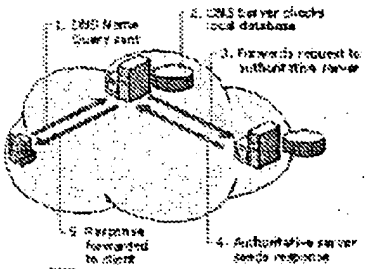
7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	
14. The method of claim 1, performed by a software module.	See claim 1, which is performed by Windows NT 4.0 at the client computer.
15. The method of claim 1, performed by a client computer.	See claim 1, which is performed by Windows NT 4.0 at the client computer.
17. A computer-readable storage medium, comprising:	Microsoft VPN, Page 11: Microsoft® Windows® NT 4.0 includes support for virtual private networking technology, which leverages the IP connectivity of the Internet to connect remote clients and remote offices. As a network professional, you should understand the important uses of virtual private networking for your organization and the underlying technologies that make it work: the Point-to-Point Tunneling Protocol (PPTP), virtual private networks and security, virtual private networks and routing and translation, virtual private networks and firewalls, and the troubleshooting of virtual private network connections. You should already be familiar with TCP/IP, IP routing, and the Windows NT 4.0 remote access server. Microsoft VPN, Page 34: 

Petitioner Apple Inc. - Exhibit 1002, p. 798

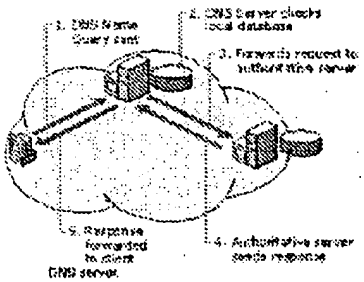
7.188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
a storage area; and	Microsoft VPN, Page 11: Microsoft® Windows® NT 4.0 includes support for virtual private networking technology, which leverages the IP connectivity of the Internet to connect remote clients and remote offices. As a network professional, you should understand the important uses of virtual private networking for your organization and the underlying technologies that make it work: the Point-to-Point Tunneling Protocol (PPTP), virtual private networks and security, virtual private networks and routing and translation, virtual private networks and firewalls, and the troubleshooting of virtual private network connections. You should already be familiar with TCP/IP, IP routing, and the Windows NT 4.0 remote access server. Microsoft VPN, Page 34: 
computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:	Microsoft VPN, Page 11: Microsoft® Windows® NT 4.0 includes support for virtual private networking technology, which leverages the IP connectivity of the Internet to connect remote clients and remote offices. As a network professional, you should understand the important uses of virtual private networking for your organization and the underlying technologies that make it work: the Point-to-Point Tunneling Protocol (PPTP), virtual private networks and security, virtual private networks and routing and translation, virtual private networks and firewalls, and the troubleshooting of virtual private network connections. You should already be familiar with TCP/IP, IP routing, and the Windows NT 4.0 remote access server. Microsoft VPN, Page 13: For the VPN connection to be established, the VPN server authenticates the VPN client attempting the connection and verifies that the VPN client has the appropriate permissions. If mutual authentication is being used, the VPN client also authenticates the VPN server, providing protection against masquerading VPN servers. Microsoft VPN, Page 34:

Petitioner Apple Inc. - Exhibit 1002, p. 799

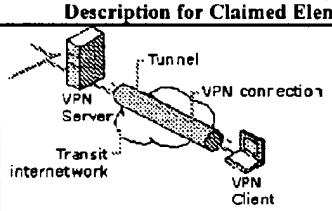
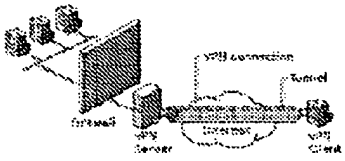
7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	
receiving a secure domain name;	Microsoft VPN, Page 32: Create a demand-dial interface for the router-to-router VPN connection with the corporate office router configured for a PPTP device, the IP address or host name of the corporate office VPN server's interface on the Internet, and a user name and password that can be verified by the VPN server. The user name must match the name of a demand-dial interface on the corporate office VPN server.
sending a query message to a secure domain name service, the query message requesting from the domain name service a secure computer network address corresponding to the secure domain name;	Microsoft VPN, Page 66:

7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	The following process outlines what happens when the DNS resolver component on a host sends a DNS query to a DNS server. This example is shown in Figure 12 and is deliberately simplified to gain a basic understanding of the DNS resolution process. 1. The DNS resolver component formats a DNS Name Query containing the FQDN and sends it to the configured DNS server.  2. The DNS server checks the FQDN in the DNS Name Query against locally stored address records. If a record is found, the IP address corresponding to the requested FQDN is sent back to the client. 3. If the FQDN is not found, the DNS server forwards the request to a DNS server that is authoritative for the FQDN. 4. The authoritative DNS server returns the reply, containing the resolved IP address, back to the original DNS server. 5. The original DNS server sends the IP address mapping information to the client.
receiving from the domain name service a response message containing the secure computer network address corresponding to the secure domain name; and	Microsoft VPN, Page 66:

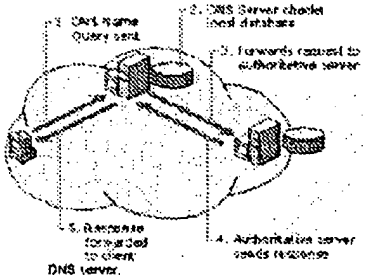
Petitioner Apple Inc. - Exhibit 1002, p. 801

7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	The following process outlines what happens when the DNS resolver component on a host sends a DNS query to a DNS server. This example is shown in Figure 15 and is deliberately simplified to gain a basic understanding of the DNS resolution process. 1. The DNS resolver component formats a DNS Name Query containing the FQDN and sends it to the configured DNS server.  2. The DNS server checks the FQDN in the DNS Name Query against locally stored address records. If a record is found, the IP address corresponding to the requested FQDN is sent back to the client. 3. If the FQDN is not found, the DNS server forwards the request to a DNS server that is authoritative for the FQDN. 4. The authoritative DNS server returns the reply, containing the resolved IP address, back to the original DNS server. 5. The original DNS server sends the IP address mapping information to the client.
sending an access request message to the secure computer network address using a virtual private network communication link.	Microsoft VPN Page 11: VPN connections allow users working at home or on the road to obtain remote access connection to an organization server using the infrastructure provided by public internetwork such as the Internet. . . . A VPN enables you to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link. Microsoft VPN Page 12:

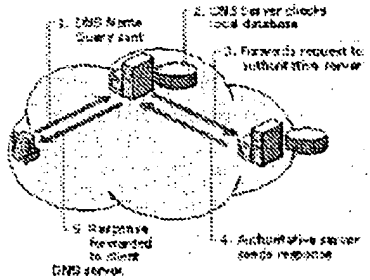
Petitioner Apple Inc. - Exhibit 1002, p. 802

7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	
26. The computer-readable medium according to claim 17, wherein the virtual private network includes the Internet.	Microsoft VPN, Page 34: 
28. The computer readable medium of claim 17, wherein the access request message contains a request for information stored at the secure computer network address.	Microsoft VPN, Page 11: A VPN enables you to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link. . . . . VPN connections allow users working at home or on the road to obtain remote access connection to an organization server using the infrastructure provided by public internetwork such as the Internet.
29. The computer-readable medium according to claim 17,	
wherein receiving the secure domain name comprises receiving the secure domain name at a client computer	Microsoft VPN, Page 32: Create a demand-dial interface for the router-to-router VPN connection with the corporate office router configured for a PPTP device. the IP address or host name of the corporate office VPN server's interface on the Internet, and a user name and password that can be verified by the VPN server. The user

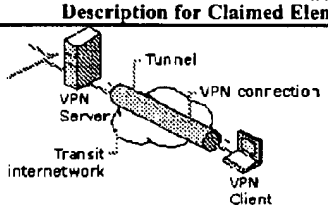
Petitioner Apple Inc. - Exhibit 1002, p. 803

7.188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
from a user;	name must match the name of a demand-dial interface on the corporate office VPN server.
wherein sending the query message comprises sending the query message at the client computer;	Microsoft VPN, Page 66: The following process outlines what happens when the DNS resolver component on a host sends a DNS query to a DNS server. This example is shown in Figure 12 and is deliberately simplified to gain a basic understanding of the DNS resolution process. 1. The DNS resolver component formats a DNS Name Query containing the FQDN and sends it to the configured DNS server.  2. The DNS server checks the FQDN in the DNS Name Query against locally stored address records. If a record is found, the IP address corresponding to the requested FQDN is sent back to the client. 3. If the FQDN is not found, the DNS server forwards the request to a DNS server that is authoritative for the FQDN. 4. The authoritative DNS server returns the reply, containing the resolved IP address, back to the original DNS server. 5. The original DNS server sends the IP address mapping information to the client.
wherein receiving the response message comprises receiving the response message at the client computer,	Microsoft VPN, Page 66:

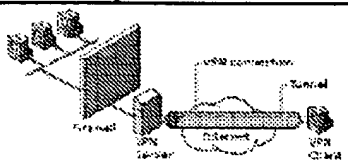
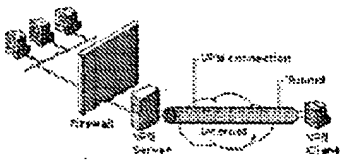
Petitioner Apple Inc. - Exhibit 1002, p. 804

7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	The following process outlines what happens when the DNS resolver component on a host sends a DNS query to a DNS server. This example is shown in Figure 12 and is deliberately simplified to gain a basic understanding of the DNS resolution process. 1. The DNS resolver component formats a DNS Name Query containing the FQDN and sends it to the configured DNS server.  2. The DNS server checks the FQDN in the DNS Name Query against locally stored address records. If a record is found, the IP address corresponding to the requested FQDN is sent back to the client. 3. If the FQDN is not found, the DNS server forwards the request to a DNS server that is authoritative for the FQDN. 4. The authoritative DNS server returns the reply, containing the resolved IP address, back to the original DNS server. 5. The original DNS server sends the IP address mapping information to the client.
wherein sending the access request message comprises sending the access request message at the client computer.	Microsoft VPN Page 11: VPN connections allow users working at home or on the road to obtain remote access connection to an organization server using the infrastructure provided by public internetwork such as the Internet. . . . A VPN enables you to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link. Microsoft VPN Page 12:

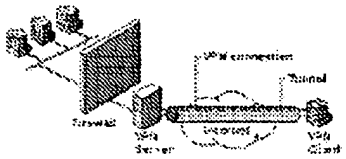
Petitioner Apple Inc. - Exhibit 1002, p. 805

7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	
30. The computer-readable medium according to claim 17, wherein the method is performed by a software module.	See claim 1, which is performed by Windows NT 4.0 at the client computer.
31. The computer-readable medium according to claim 17, wherein the method is performed by a client computer.	See claim 1, which is performed by Windows NT 4.0 at the client computer.
33. A data processing apparatus, comprising:	Microsoft VPN, Page 11: Microsoft® Windows® NT 4.0 includes support for virtual private networking technology, which leverages the IP connectivity of the Internet to connect remote clients and remote offices. As a network professional, you should understand the important uses of virtual private networking for your organization and the underlying technologies that make it work: the Point-to-Point Tunneling Protocol (PPTP), virtual private networks and security, virtual private networks and routing and translation, virtual private networks and firewalls, and the troubleshooting of virtual private network connections. You should already be familiar with TCP/IP, IP routing, and the Windows NT 4.0 remote access server. Microsoft VPN, Page 34:

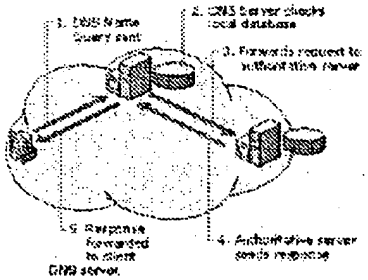
Petitioner Apple Inc. - Exhibit 1002, p. 806

7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	
a processor, and	Microsoft VPN, Page 11: Microsoft® Windows® NT 4.0 includes support for virtual private networking technology, which leverages the IP connectivity of the Internet to connect remote clients and remote offices. As a network professional, you should understand the important uses of virtual private networking for your organization and the underlying technologies that make it work: the Point-to-Point Tunneling Protocol (PPTP), virtual private networks and security, virtual private networks and routing and translation, virtual private networks and firewalls, and the troubleshooting of virtual private network connections. You should already be familiar with TCP/IP, IP routing, and the Windows NT 4.0 remote access server. Microsoft VPN, Page 34: 
memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:	Microsoft VPN, Page 11: Microsoft® Windows® NT 4.0 includes support for virtual private networking technology, which leverages the IP connectivity of the Internet to connect remote clients and remote offices. As a network professional, you should understand the important uses of virtual private networking for your organization and the underlying technologies that make it work: the Point-to-Point Tunneling Protocol (PPTP), virtual private networks and security, virtual private networks and routing and translation, virtual private networks and firewalls, and the troubleshooting of virtual private network connections. You should already be familiar with TCP/IP, IP routing, and the Windows NT 4.0 remote access server.

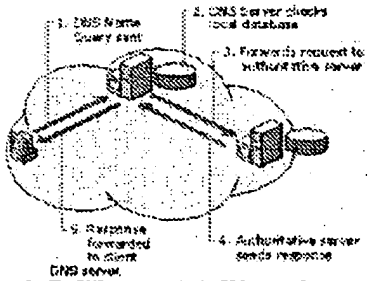
Petitioner Apple Inc. - Exhibit 1002, p. 807

7.188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	Microsoft VPN, Page 13: For the VPN connection to be established, the VPN server authenticates the VPN client attempting the connection and verifies that the VPN client has the appropriate permissions. If mutual authentication is being used, the VPN client also authenticates the VPN server, providing protection against masquerading VPN servers. Microsoft VPN, Page 34:  Figure 13: VPN Server on the Internet in Front of the Firewall
receiving a secure domain name;	Microsoft VPN, Page 32: Create a demand dial interface for the router to router VPN connection with the corporate office router configured for a PPTP device, the IP address or host name of the corporate office VPN server's interface on the Internet, and a user name and password that can be verified by the VPN server. The user name must match the name of a demand-dial interface on the corporate office VPN server.
sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name;	Microsoft VPN, Page 66:

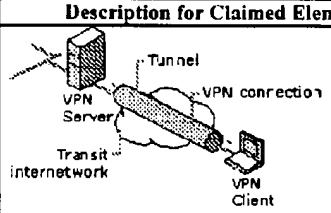
Petitioner Apple Inc. - Exhibit 1002, p. 808

7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	The following process outlines what happens when the DNS resolver component on a host sends a DNS query to a DNS server. This example is shown in Figure 12 and is deliberately simplified to gain a basic understanding of the DNS resolution process. 1. The DNS resolver component formats a DNS Name Query containing the FQDN and sends it to the configured DNS server.  2. The DNS server checks the FQDN in the DNS Name Query against locally stored address records. If a record is found, the IP address corresponding to the requested FQDN is sent back to the client. 3. If the FQDN is not found, the DNS server forwards the request to a DNS server that is authoritative for the FQDN. 4. The authoritative DNS server returns the reply, containing the resolved IP address, back to the original DNS server. 5. The original DNS server sends the IP address mapping information to the client.
receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and	Microsoft VPN, Page 66:

Petitioner Apple Inc. - Exhibit 1002, p. 809

7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	The following process outlines what happens when the DNS resolver component on a host sends a DNS query to a DNS server. This scenario is shown in Figure 12 and is deliberately simplified to gain a basic understanding of the DNS resolution process. 1. The DNS resolver component formats a DNS Name Query containing the FQDN and sends it to the configured DNS server.  2. The DNS server checks the FQDN in the DNS Name Query against locally stored address records. If a record is found, the IP address corresponding to the requested FQDN is sent back to the client. 3. If the FQDN is not found, the DNS server forwards the request to a DNS server that is authoritative for the FQDN. 4. The authoritative DNS server returns the reply, containing the resolved IP address, back to the original DNS server. 5. The original DNS server sends the IP address mapping information to the client.
sending an access request message to the secure computer network address using a virtual private network communication link.	Microsoft VPN Page 11: VPN connections allow users working at home or on the road to obtain remote access connection to an organization server using the infrastructure provided by public internetwork such as the Internet. . . . A VPN enables you to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link. Microsoft VPN Page 12:

Petitioner Apple Inc. - Exhibit 1002, p. 810

7,188,180 Claim Elements	Description for Claimed Elements in the Microsoft VPN Prior Art Reference
	

3-26-12 TFV

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

OPAP IAP23 MAR 23 2012 PATENT & TRADEMARK OFFICE

CERTIFICATION STATEMENT

[X] Under 37 C.F.R. 1.98(d), copies of all patent, publication, pending U.S. application or other information that was previously submitted to, or cited by the USPTO in an earlier application are not required. Applicant will provide copies of the previously submitted references at the Examiner's request. **Enclosed are copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).**

This application claims priority from and is a continuation of a co-pending U.S. Application No. 13/049,552, filed March 16, 2011, which is a continuation of U.S. Application No. 11/840,560, filed August 17, 2007, now U.S. Patent No. 7,921,211, which is a continuation of U.S. Application No. 10/714,849, filed November 18, 2003, now U.S. Patent No. 7,418,504, which is a continuation of U.S. Application No. 09/558,210, filed April 26, 2000, now abandoned, which is a continuation-in-part of U.S. Application No. 09/504,783, filed on February 15, 2000, now U.S. Patent No. 6,502,135, issued December 31, 2002.

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[ ] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[X] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Date: 3/22/12

03/27/2012 HVUONG1 00000012 501133 13336790
01 FC:1806 180.00 DA

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

DM_US 32511456-1.077580.0151

OPAP IAP23
MAR 23 2012
PATENT & TRADEMARK OFFICE

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

OPAP
MAR 2 3 2012
IAP23
PATENT & TRADEMARK OFFICE

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc Code: TRAN.LET

Document Description: Transmittal Letter

OPAP 23
MAR 23 2012
PATENT & TRADEMARK OFFICE

PTO/SB/21 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission	52

Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Attorney Docket Number	077580-0151 (VRNK-0001CP3CNFT1)

ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
  - [x] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [x] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [x] Other Enclosure(s) (please Identify below):

Remarks

16 Boxes which include copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	McDermott, Will and Emery		
Signature			
Printed name	Toby H. Kusmer		
Date	March 23, 2012	Reg. No.	26,408

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name		Date	

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

OPAP IAP23 MAR 23 2012 PATENT & TRADEMARK OFFICE

PTO/SB/17 (09-11)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

FEE TRANSMITTAL

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT	($)	180.00

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Examiner Name	Krisna Lim
Art Unit	2453
Attorney Docket No.	77580-151 VRNK-0001CP3CNFT1

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☑ Deposit Account Deposit Account Number: 50-1133 Deposit Account Name: McDermott, Will and Emery

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☑ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**

☑ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☐ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

Application Type	FILING FEES Fee ($)	FILING FEES Small Entity Fee ($)	SEARCH FEES Fee ($)	SEARCH FEES Small Entity Fee ($)	EXAMINATION FEES Fee ($)	EXAMINATION FEES Small Entity Fee ($)	Fees Paid ($)
Utility	380	190	620	310	250	125	
Design	250	125	120	60	160	80	
Plant	250	125	380	190	200	100	
Reissue	380	190	620	310	750	375	
Provisional	250	125	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	60	30
Each independent claim over 3 (including Reissues)	250	125
Multiple dependent claims	450	225

Total Claims _____ - 20 or HP = _____ x _____ = _____ Extra Claims / Fee ($) / Fee Paid ($)

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims _____ - 3 or HP = _____ x _____ = _____ Extra Claims / Fee ($) / Fee Paid ($)

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims Fee ($) _____ Fee Paid ($) _____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets _____ - 100 = _____ Extra Sheets / 50 = _____ Number of each additional 50 or fraction thereof (round up to a whole number) x _____ Fee ($) = _____ Fee Paid ($)

4. OTHER FEE(S)

	Fees Paid ($)
Non-English Specification, $130 fee (no small entity discount)	
Other (e.g., late filing surcharge): Information Disclosure Statement Filing Fee	$180.00

SUBMITTED BY

Signature		Registration No. (Attorney/Agent) 26,418	Telephone 617-535-4000
Name (Print/Type)	Toby H. Kusmer		Date March 23, 2012

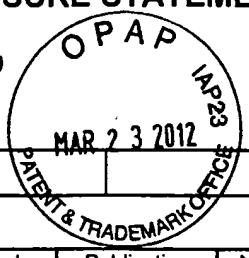
This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)



Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Patent Number	Patent Date	Inventor	
	A1	09/399,753	09/22/1998	Graig Miller et al.	
	A2	2,895,502	07/21/1959	Roper et al.	
	A3	4,761,334	08/1988	Sagoi et al.	
	A4	4,885,778	12/5/1989	Weiss, Kenneth	
	A5	4,920,484	4/24/1990	Ranade	
	A6	4,933,846	06/12/1990	Humphrey et al.	
	A7	4,952,930	08/28/1990	Franaszek et al.	
	A8	4,988,990	01/29/1991	Warrior	
	A9	5,164,988	11/17/1992	Matyas	
	A10	5,204,961	04/20/1993	Barlow	
	A11	5,276,735	01/04/1994	Boebert et al	
	A12	5,303,302	04/12/1994	Burrows	
	A13	5,311,593	05/10/1994	Carmi	
	A14	5,329,521	07/12/1994	Walsh et al.	
	A15	5,341,426	08/23/1994	Barney et al.	
	A16	5,367,643	11/22/1994	Chang et al	
	A17	5,384,848	01/24/1995	Kikuchi	
	A18	5,511,122	04/23/1996	Atkinson	
	A19	5,548,646	08/20/1996	Aziz et al.	
	A20	5,559,883	09/24/1996	Williams	
	A21	5,561,669	10/01/1996	Lenney et al	
	A22	5,588,060	12/24/1996	Aziz	
	A23	5,590,285	12/31/1996	Krause et al.	
	A24	5,625,626	04/29/1997	Umekita	
	A25	5,629,984	05/13/1997	McManis	
	A26	5,654,695	08/05/1997	Olnowich et al	
	A27	5,682,480	10/28/1997	Nakagawa	
	A28	5,689,566	11/18/1997	Nguyen	
	A29	5,689,641	11/18/1997	Ludwig et al.	
	A30	5,740,375	04/14/1998	Dunne et al.	
	A31	5,757,925	05/1998	Faybishenko	
	A32	5,764,906	06/1998	Edelstein et al.	
	A33	5,771,239	06/23/1998	Moroney et al.	
	A34	5,774,660	6/30/1998	Brendel et al	
	A35	5,787,172	07/28/1998	Arnold	
	A36	5,790,548	08/04/1998	Sitaraman et al.	
	A37	5,796,942	08/18/1998	Esbensen	
	A38	5,805,801	09/08/1998	Holloway et al.	
	A39	5,805,803	09/08/1998	Birrell et al.	
	A40	5,822,434	10/13/1998	Caronni et al.	
	A41	5,842,040	11/24/1998	Hughes et al.	
	A42	5,845,091	12/01/1998	Dunne et al.	
	A43	5,864,666	01/1999	Shrader, Theodore Jack London	
	A44	5,867,650	02/02/1998	Osterman	
	A45	5,870,610	02/09/1999	Beyda et al.	
	A46	5,878,231	05/02/1999	Baehr et al	
	A47	5,892,903	04/06/1999	Klaus	
	A48	5,898,830	04/27/1999	Wesinger, Jr. et al.	
	A49	5,905,859	05/18/1999	Holloway et al.	
	A50	5,918,018	06/29/1999	Gooderum et al.	

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

	A51		5,918,019	06/29/1999	Valencia	
	A52		5,950,195	09/07/1999	Stockwell et al.	
	A53		5,950,519	09/14/1999	Anatoli	
	A54		5,960,204	09/28/1999	Yinger et al.	
	A55		5,996,016	11/30/1999	Thalheimer et al.	
	A56		6,006,259	12/21/1999	Adelman et al.	
	A57		6,006,272	12/21/1999	Aravamudan et al	
	A58		6,016,318	01/18/2000	Tomoike	
	A59		6,016,512	01/18/2000	Huitema	
	A60		6,041,342	03/21/2000	Yamaguchi	
	A61		6,052,788	04/2000	Wesinger et al.	
	A62		6,055,574	04/25/2000	Smorodinsky et al.	
	A63		6,061,346	05/2000	Nordman, Mikael	
	A64		6,061,736	05/09/2000	Rochberger et al	
	A65		6,079,020	06/20/2000	Liu	
	A66		6,081,900	06/2000	Subramaniam et al.	
	A67		6,092,200	07/18/2000	Muniyappa et al.	
	A68		6,101,182	08/2000	Sistanizadeh et al.	
	A69		6,119,171	09/12/2000	Alkhatib	
	A70		6,119,234	09/12/2000	Aziz et al.	
	A71		6,147,976	11/14/2000	Shand et al.	
	A72		6,157,957	12/05/2000	Berthaud	
	A73		6,158,011	12/05/2000	Chen et al.	
	A74		6,168,409	01/02/2001	Fare	
	A75		6,173,399	01/09/2001	Gilbrech	
	A76		6,175,867	01/16/2001	Taghadoss	
	A77		6,178,409	01/23/2001	Weber et al.	
	A78		6,178,505	01/23/2001	Schneider et al	
	A79		6,179,102	01/30/2001	Weber, et al.	
	A80		6,182,141	1/30/2001	Blum et al.	
	A81		6,199,112	03/2001	Wilson, Stephen K.	
	A82		6,202,081	03/2001	Naudus, Stanley T.	
	A83		6,222,842	04/24/2001	Sasyan et al.	
	A84		6,223,287	04/24/2001	Douglas et al.	
	A85		6,226,748	05/01/2001	Bots et al.	
	A86		6,226,751	05/01/2001	Arrow et al..	
	A87		6,233,618	05/15/2001	Shannon	
	A88		6,243,360	06/05/2001	Basilico	
	A89		6,243,749	06/05/2001	Sitaraman et al.	
	A90		6,243,754	06/05/2001	Guerin et al	
	A91		6,246,670	06/12/2001	Karlsson et al.	
	A92		6,256,671	07/03/2001	Strentzsch et al.	
	A93		6,262,987	07/17/01	Mogul, Jeffrey C.	
	A94		6,263,445	07/17/2001	Blumenau	
	A95		6,269,099	07/31/2001	Borella et al.	
	A96		6,286,047	09/04/2001	Ramanathan et al	
	A97		6,298,341	10/02/01	Mann, et al.	
	A98		6,301,223	10/9/2001	Hrastar et al	
	A99		6,308,213	10/23/2001	Valencia	
	A100		6,308,274	10/23/2001	Swift	
	A101		6,311,207	10/30/2001	Mighdoll et al	
	A102		6,314,463	11/2001	Abbott et al.	
	A103		6,324,161	11/27/2001	Kirch	
	A104		6,330,562	12/11/2001	Boden et al.	
	A105		6,332,158	12/18/2001	Risley et al.	
	A106		6,333,272	12/25/01	McMillin, et al.	
	A107		6,338,082	01/08/02	Schneider, Eric	

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

	A108		6,353,614	03/05/2002	Borella et al.	
	A109		6,425,003	07/23/2002	Herzog et al.	
	A110		6,430,155	08/06/2002	Davie et al	
	A111		6,430,610	08/06/2002	Carter	
	A112		6,487,598	11/26/2002	Valencia	
	A113		6,496,867	12/17/2002	Beser et al.	
	A114		6,502,135	12/2002	Munger et al.	
	A115		6,505,232	01/07/2003	Mighdoll et al	
	A116		6,510,154	01/21/2003	Mayes et al	
	A117		6,549,516	04/15/2003	Albert et al	
	A118		6,557,037	04/2003	Provino, Joseph E.	
	A119		6,560,634	05/06/2003	Broadhurst	
	A120		6,571,296	05/27/2002	Dillon	
	A121		6,571,338	05/27/2003	Shaio et al.	
	A122		6,581,166	7/17/2003	Hirst et al.	
	A123		6,606,708	08/12/2003	Devine et al.	
	A124		6,615,357	9/2/2003	Boden et al.	
	A125		6,618,761	09/09/2003	Munger et al.	
	A126		6,671,702	12/30/2003	Kruglikov et al	
	A127		6,687,551	2/3/2004	Steindl	
	A128		6,687,746	02/03/04	Shuster, et al.	
	A129		6,701,437	03/02/2004	Hoke et al.	
	A130		6,714,970	3/30/2004	Fiveash et al.	
	A131		6,717,949	4/6/2004	Boden et al.	
	A132		6,751,738	06/15/2004	Wesinger, Jr. et al..	
	A133		6,752,166	06/22/04	Lull, et al.	
	A134		6,757,740	06/29/04	Parekh, et al.	
	A135		6,760,766	7/6/2004	Sahlqvist	
	A136		6,813,777	11/2004	Weinberger et al.	
	A137		6,826,616	11/30/2004	Larson et al.	
	A138		6,839,759	1/4/2005	Larson et al.	
	A139		6,937,597	08/30/2005	Rosenberg et al.	
	A140		60/134,547	05/17/1999	Victory Sheymov	
	A141		60/151,563	08/31/1999	Bryan Whittles	
	A142		7,010,604	3/7/2006	Munger et al.	
	A143		7,039,713	05/2006	Van Gunter et al.	
	A144		7,072,964	07/04/2006	Whittle et al.	
	A145		7,133,930	11/7/2006	Munger et al.	
	A146		7,167,904	01/23/07	Devarajan, et al.	
	A147		7,188,175	03/06/07	McKeeth, James A.	
	A148		7,188,180	3/6/2007	Larson et al.	
	A149		7,197,563	3/27/2007	Sheymov et al.	
	A150		7,353,841	04/08/08	Kono, et al.	
	A151		7,418,504	08/2008	Larson et al.	
	A152		7,461,334	12/02/08	Lu, et al.	
	A153		7,490,151	02/2009	Munger et al.	
	A154		7,493,403	02/2009	Shull et al.	
	A155		7,584,500	09/2009	Dillon et al.	
	A156		7,764,231	07/27/2010	Karr et al.	
	A157		7,852,861	12/2010	Wu et al.	
	A158		7,921,211	04/2011	Larson et al.	
	A159		7,933,990	04/2011	Munger et al.	
	A160		8,051,181	11/2011	Larson et al.	

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	B1	US2001/0049741	12/2001	Skene et al.	
	B2	US2002/0004898	1/10/02	Droge	
	B3	US2003/0196122	10/16/2003	Wesinger, Jr. et al.	
	B4	US2004/0199493	10/2004	Ruiz et al.	
	B5	US2004/0199520	10/2004	Ruiz et al.	
	B6	US2004/0199608	10/2004	Rechterman et al.	
	B7	US2004/0199620	10/2004	Ruiz et al.	
	B8	US2005/0055306	3/10/05	Miller et al.	
	B9	US2005/0108517	05/2005	Dillon et al.	
	B10	US2006/0059337	03/16/2006	Polyhonen et al.	
	B11	US2006/0123134	06/2006	Munger et al.	
	B12	US2007/0208869	09/2007	Adelman et al.	
	B13	US2007/0214284	09/2007	King et al.	
	B14	US2007/0266141	11/2007	Norton, Michael Anthony	
	B15	US2008/0005792	01/2008	*Larson et al.	
	B16	US2008/0144625	06/2008	Wu et al.	
	B17	US2008/0235507	09/2008	Ishikawa et al.	
	B18	US2009/0193498	07/2009	Agarwal et al.	
	B19	US2009/0193513	07/2009	Agarwal et al.	
	B20	US2009/0199258	08/2009	Deng et al.	
	B21	US2009/0199285	09/2009	Agarwal et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3 – Number 4 –Kind Code5 (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No
	C1	DE19924575	12/2/99	Provino et al.			
	C2	EP0814589	12/29/1997	AT&T Corp.			
	C3	EP0838930	4/29/1988	Digital Equipment Corporation			
	C4	EP0858189	8/12/98	Maciel et al.			
	C5	EP836306	4/15/1998	HEWLETT PACKARD CO			
	C6	GB2317792	04/01/1998	Secure Computing Corporation			
	C7	GB2334181	08/11/1999	NEC Technologies			
	C8	GB2340702	02/23/2000	Sun Microsystems Inc.			
	C9	JP04-363941	12/16/1992	Nippon Telegr & Teleph Corp			
	C10	JP09-018492	01/17/1997	Nippon Telegr & Teleph Corp			
	C11	JP10-070531	03/10/1998	Brother Ind Ltd.			
	C12	JP62-214744	9/21/1987	Hitachi Ltd.			
	C13	WO0070458	11/23/2000	Comsec Corporation			
	C14	WO0017775	3/30/00	Miller et al.			
	C15	WO01016766	03/08/2001	Science Applications International Corporation			
	C16	WO0150688	7/12/01	Kriens			
	C17	WO9827783	06/25/1998	Northern Telecom Limited			
	C18	WO9855930	12/10/98	Tang			

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

	C19	WO9843396	10/01/1998	Northern Telecom Limited			
	C20	WO9859470	12/30/98	Kanter et al.			
	C21	WO9911019	03/04/1999	V One Corp			
	C22	WO9938081	7/29/99	Paulsen et al.			
	C23	WO9948303	9/23/99	Cox et al.			
	C24	WO01/61922	02/12/2001	Science Application International Corporation			

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D1	Alan 0. Frier et al., "The SSL Protocol Version 3.0", Nov. 18, 1996, printed from http://www.netscape.com/eng/ss13/ draft302.txt on Feb. 4, 2002, 56 pages.	
	D2	August Bequai, "Balancing Legal Concerns Over Crime and Security in Cyberspace", Computer & Security, vol. 17, No. 4, 1998, pp. 293-298.	
	D3	D. B. Chapman et al., "Building Internet Firewalls", Nov. 1995, pp. 278-375.	
	D4	D. Clark, "US Calls for Private Domain-Name System", Computer, IEEE Computer Society, Aug. 1, 1998, pp. 22-25.	
	D5	Davila J et al, "Implementation of Virtual Private Networks at the Transport Layer", Information Security, Second International Work-shop, ISW'99. Proceedings (Lecture Springer-Verlag Berlin, Germany, [Online] 1999, pp. 85-102, XP002399276, ISBN 3-540-666	
	D6	Dolev, Shlomi and Ostrovsky, Rafil, "Efficient Anonymous Multicast and Reception" (Extended Abstract), 16 pages.	
	D7	Donald E. Eastlake, 3rd, "Domain Name System Security Extensions", INTERNET DRAFT, Apr. 1998, pp. 1-51.	
	D8	F. Halsall, "Data Communications, Computer Networks and Open Systems", Chapter 4, Protocol Basics, 1996, pp. 198-203.	
	D9	Glossary for the Linux FreeS/WAN project, printed from http://liberty.freeswan.org/freeswan_trees/freeswan-1.3/ doc/glossary.html on Feb. 21, 2002, 25 pages.	
	D10	J. Gilmore, "Swan: Securing the Internet against Wiretapping", printed from http://liberty.freeswan.org/freeswan _trees/freeswan-1.3/doc/rationale.html on Feb. 21, 2002, 4 pages.	
	D11	James E. Bellaire, "New Statement of Rules-Naming Internet Domains", Internet Newsgroup, Jul. 30, 1995, 1 page.	
	D12	Jim Jones et al., "Distributed Denial of Service Attacks: Defenses", Global Integrity Corporation, 2000, pp. 1-14.	
	D13	Laurie Wells (LANCASTERBIBELMAIL MSN COM); "Subject: Security Icon" USENET Newsgroup, Oct. 19, 1998, XP002200606, 1 page.	
	D14	Linux FreeS/WAN Index File, printed from http://liberty.freewan.org/freeswan_trees/freeswan-1.3/doc/ on Feb. 21, 2002, 3 Pages.	
	D15	P. Srisuresh et al., "DNS extensions to Network address Translators (DNS_ALG)", Internet Draft, Jul. 1998, pp. 1-27.	
	D16	Reiter, Michael K. and Rubin, Aviel D. (AT&T Labs-Research), "Crowds: Anonymity for Web Transactions", pp. 1-23.	
	D17	RFC 2401 (dated Nov. 1998) Security Architecture for the Internet Protocol (RTP)	
	D18	RFC 2543-SIP (dated March 1999): Session Initiation Protocol (SIP or SIPS)	
	D19	Rich Winkel, "CAQ: Networking With Spooks: The NET & The Control Of Information", Internet Newsgroup, Jun. 21, 1997, 4 pages.	
	D20	Rubin, Aviel D., Geer, Daniel, and Ranum, Marcus J. (Wiley Computer Publishing), "Web Security Sourcebook", pp. 82-94.	
	D21	Search Report (dated Aug. 20, 2002), International Application No. PCT/US01/04340.	
	D22	Search Report (dated Aug. 23, 2002), International Application No. PCT/US01/13260.	
	D23	Search Report (dated Oct. 7, 2002), International Application No. PCT/US01/13261.	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

	D24	Search Report, IPER (dated Nov. 13, 2002), International Application No. PCT/US01/04340.	
	D25	Search Report, IPER (dated Feb. 06, 2002), International Application No. PCT/US01/13261.	
	D26	Search Report, IPER (dated Jan. 14, 2003), International Application No. PCT/US01/13260.	
	D27	Shankar, A.U. "A verified sliding window protocol with variable flow control". Proceedings of ACM SIGCOMM conference on Communications architectures & protocols. pp. 84-91, ACM Press, NY, NY 1986.	
	D28	Shree Murthy et al., "Congestion-Oriented Shortest Multi-path Routing", Proceedings of IEEE INFOCOM, 1996, pp. 1028-1036.	
	D29	W. Stallings, "Cryptography And Network Security", 2nd, Edition, Chapter 13, IP Security, Jun. 8, 1998, pp. 399-440.	
	D30	Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009, VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation.	
	D31	Appendix A of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	D32	Concordance Table For the References Cited in Tables on pages 6-15, 71-80 and 116-124 of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	D33	1. P. Mockapetris, "DNS Encoding of Network Names and Other Types," Network Working Group, RFC 1101 (April 1989) RFC1101, DNS SRV)	
	D34	R. Atkinson, "An Internetwork Authentication Architecture," Naval Research Laboratory, Center for High Assurance Computing Systems (8/5/93). (Atkinson NRL, KX Records)	
	D35	Henning Schulzrinne, *Personal Mobility For Multimedia Services In The Internet*, Proceedings of the Interactive Distributed Multimedia Systems and Services European Workshop at 143 (1996). (Schulzrinne 96)	
	D36	Microsoft Corp., *Microsoft Virtual Private Networking: Using Point-to-Point Tunneling Protocol for Low-Cost, Secure, Remote Access Across the Internet* (1996) (printed from 1998 PDC DVD-ROM). (Point to Point, Microsoft Prior Art VPN Technology)	
	D37	"Safe Surfing: How to Build a Secure World Wide Web Connection," IBM Technical Support Organization, (March 1996). (Safe Surfing, WEBSITE ART)	
	D38	Goldschlag, et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK (May 1996). (Goldschlag II, Onion Routing)	
	D39	"IPSec Minutes From Montreal", IPSEC Working Group Meeting Notes, http://www.sandleman.ca/ipsec/1996/08/msg00018.html (June 1996). (IPSec Minutes, FreeS/WAN)	
	D40	J. M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California, July 1996. (Galvin, DNSSEC)	
	D41	J. Gilmore, et al. "Re: Key Management, anyone? (DNS Keying)," IPSec Working Group Mailing List Archives (8/96). (Gilmore DNS, FreeS/WAN)	
	D42	H. Orman, et al. "Re: 'Re: DNS? was Re: Key Management, anyone?" IETF IPSec Working Group Mailing List Archive (8/96-9/96). (Orman DNS, FreeS/WAN)	
	D43	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2052 (October 1996). (RFC 2052, DNS SRV)	
	D44	Freier, et al. "The SSL Protocol Version 3.0," Transport Layer Security Working Group (November 18, 1996). (SSL, UNDERLYING SECURITY TECHNOLOGY)	
	D45	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/02/1996). (RFC 2543 Internet Draft 1)	
	D46	M.G. Reed, et al. "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA, Dec. 9-13, 1996. (Reed, Onion Routing)	
	D47	Kenneth F. Alden & Edward P. Wobber, *The AltaVista Tunnel: Using the Internet to Extend Corporate Networks*, Digital Technical Journal (1997) (Alden, AltaVista)	
	D48	Automotive Industry Action Group, "ANX Release 1 Document Publication," AIAG (1997). (AIAG, ANX)	
	D49	Automotive Industry Action Group, "ANX Release 1 Draft Document Publication," AIAG Publications (1997). (AIAG Release, ANX)	
	D50	Aventail Corp. "Aventail VPN Data Sheet," *available at* http://www.archive.org/web/19970212013043/www.aventail.com/prod/vpndata.html (1997). (Data Sheet, Aventail)	
	D51	Aventail Corp., "Directed VPN Vs. Tunnel," *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/directvpn.html (1997). (Directed VPN, Aventail)	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

	D52	Aventail Corp., "Managing Corporate Access to the Internet," Aventail AutoSOCKS White Paper *available at* http://web.archive.org/19970620030031 2/www.aventail.com/educate/whitepaper/ipmw.html (1997). (Corporate Access, Aventail)	
	D53	Aventail Corp., "VPN Server V2.0 Administration Guide," (1997). (VPN, Aventail)	
	D54	Goldschlag, et al. "*Privacy on the Internet*," Naval Research Laboratory, Center for High Assurance Computer Systems (1997). (Goldschtag I, Onion Routing)	
	D55	Microsoft Corp., *Installing Configuring and Using PPTP with Microsoft Clients and Servers* (1997). (Using PPTP, Microsoft Prior Art VPN Technology)	
	D56	Microsoft Corp., *IP Security for Microsoft Windows NT Server 5.0* (1997) (printed from 1998 PDC DVD-ROM). (IP Security, Microsoft Prior Art VPN Technology)	
	D57	Microsoft Corp., *Microsoft Windows NT Active Directory: An Introduction to the Next Generation Directory Services* (1997) (printed from 1998 PDC DVD-ROM). (Directory, Microsoft Prior Art VPN Technology)	
	D58	Microsoft Corp., *Routing and Remote Access Service for Windows NT Server New Opportunities Today and Looking Ahead* (1997) (printed from 1998 PDC DVD-ROM). Routing, Microsoft Prior Art VPN Technology)	
	D59	Microsoft Corp., *Understanding Point-to-Point Tunneling Protocol PPTP* (1997) (printed from 1998 PDC DVD-ROM). (Understanding PPTP, Microsoft Prior Art VPN Technology)	
	D60	J. Mark Smith et.al., *Protecting a Private Network: The AltaVista Firewall*, Digital Technical Journal (1997). (Smith, AltaVista)	
	D61	Naganand Doraswamy *Implementation of Virtual Private Networks (VPNs) with IPSecurity*, <draft-ietf-ipsec-vpn-00.txt> (March 12, 1997). (Doraswamy)	
	D62	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (03/27/1997). (RFC 2543 Internet Draft 2)	
	D63	Aventail Corp., "Aventail and Cybersafe to Provide Secure Authentication For Internet and Intranet Communication," Press Release, April 3, 1997. (Secure Authentication, Aventail)	
	D64	D. Wagner, et al. "Analysis of the SSL 3.0 Protocol," (April 15, 1997). (Analysis, UNDERLYING SECURITY TECHNOLOGIES)	
	D65	Automotive Industry Action Group, "ANXO Certification Authority Service and Directory Service Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Definition, ANX)	
	D66	Automotive Industry Action Group, "ANXO Certification Process and ANX Registration Process Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Certification, ANX)	
	D67	Aventail Corp., "Aventail Announces the First VPN Solution to Assure Interoperability Across Emerging Security Protocols," June 2, 1997. (First VPN, Aventail)	
	D68	Syverson, et al. "Private Web Browsing," Naval Research Laboratory, Center for High 8 Assurance Computer Systems (June 2, 1997). (Syverson, Onion Routing)	
	D69	Bellcore, "Metrics, Criteria, and Measurement Technique Requirements for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (June 16, 1997). (AIAG Requirements, ANX)	
	D70	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/31/1997). (RFC 2543 Internet Draft 3)	
	D71	R. Atkinson, "Key Exchange Delegation Record for the DNS," Network Working Group, RFC 2230 (November 1997). (RFC 2230, KX Records)	
	D72	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/11/1997). (RFC 2543 Internet Draft 4)	
	D73	1998 Microsoft Professional Developers Conference DVD ("1998 PDC DVD-ROM") (including screenshots captured there from and produced as MSFTVX 00018827-00018832). (Conference, Microsoft Prior Art VPN Technology)	
	D74	Microsoft Corp., *Virtual Private Networking An Overview* (1998) (printed from 1998 PDC DVD-ROM) (Overview, Microsoft Prior Art VPN Technology)	
	D75	Microsoft Corp., *Windows NT 5.0 Beta Has Public Premiere at Seattle Mini-Camp Seminar attendees get first look at the performance and capabilities of Windows NT 5.0* (1998) (*available at* http://www.microsoft.com/presspass/features/1998/10-19nt5.mspxpftrue). (NT Beta, Microsoft Prior Art VPN Technology)	
	D76	"What ports does SSL use" *available at* stason.org/TULARC/security/ssl-talk/3-4-What-ports-does-ssl-use.html (1998). (Ports, DNS SRV)	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

	D77	Aventail Corp., "Aventail VPN V2.6 Includes Support for More Than Ten Authentication Methods Making Extranet VPN Development Secure and Simple," Press Release, January 19, 1998. (VPN V2.6, Aventail)	
	D78	R. G. Moskowitz, "Network Address Translation Issues with IPsec," Internet Draft, Internet Engineering Task Force, February 6, 1998. (Moskowitz)	
	D79	H. Schulzrinne, et al, "Internet Telephony Gateway Location," Proceedings of IEEE INfocom '98, The Conference on Computer Communications, Vol. 2 (March 29 – April 2, 1998). (Gateway, Schulzrinne)	
	D80	C. Huitema, 45 al. "Simple Gateway Control Protocol," Version 1.0 (May 5, 1998). (SGCP)	
	D81	DISA "Secret Internet Protocol Router Network," SIPRNET Program Management Office (D3113) DISN Networks, DISN Transmission Services (May 8, 1998). DISA, SIPRNET)	
	D82	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (05/14/1998). (RFC 2543 Internet Draft 5)	
	D83	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (06/17/1998). (RFC 2543 Internet Draft 6)	
	D84	D. McDonald, et al. "PF_KEY Key Management API, Version 2," Network Working Group, RFC 2367 (July 1998). (RFC 2367)	
	D85	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/16/1998). (RFC 2543 Internet Draft 7)	
	D86	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (08/07/1998). (RFC 2543 Internet Draft 8)	
	D87	Microsoft Corp., *Company Focuses on Quality and Customer Feedback* (August 18, 1998). (Focus, Microsoft Prior Art VPN Technology)	
	D88	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (09/18/1998). (RFC 2543 Internet Draft 9)	
	D89	Atkinson, et al. "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998). (RFC 2401, UNDERLYING SECURITY TECHNOLOGIES)	
	D90	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/12/1998). (RFC 2543 Internet Draft 10)	
	D91	Donald Eastlake, *Domain Name System Security Extensions*, IETF DNS Security Working Group (December 1998). (DNSSEC-7)	
	D92	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/15/1998). (RFC 2543 Internet Draft 11)	
	D93	Aventail Corp., "Aventail Connect 3.1/2.6 Administrator's Guide," (1999). (Aventail Administrator 3.1, Aventail)	
	D94	Aventail Corp., "Aventail Connect 3.1/2.6 User's Guide," (1999). (Aventail User 3.1, Aventail)	
	D95	Aventail Corp., "Aventail ExtraWeb Server v3.2 Administrator's Guide," (1999). (Aventail ExtraWeb 3.2, Aventail)	
	D96	Kaufman et al, "Implementing IPsec," (Copyright 1999). (Implementing IPSEC, VPN REFERENCES)	
	D97	Network Solutions, Inc. "Enabling SSL," NSI Registry (1999). (Enabling SSL, UNDERLYING SECURITY TECHNOLOGIES)	
	D98	Check Point Software Technologies Ltd. (1999) (Check Point, Checkpoint FW)	
	D99	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*,<draft-ietf-dnsind-frc2052bis-02.txt> (January 1999). (Gulbrandsen 99, DNS SRV)	
	D100	C. Scott, et al. *Virtual Private Networks*, O'Reilly and Associates, Inc., 2nd ed. (Jan. 1999). Scott VPNs)	
	D101	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (01/15/1999). (RFC 2543 Internet Draft 12)	
	D102	Goldschlag, et al., "Onion Routing for Anonymous and Private Internet Connections," Naval Research Laboratory, Center for High Assurance Computer Systems (January 28, 1999). (Goldschlag III, Onion Routing)	
	D103	H. Schulzrinne, "Internet Telephony: architecture and protocols – an IETF perspective," Computer Networks, Vol. 31, No. 3 (February 1999). (Telephony, Schulzrinne)	
	D104	M. Handley, et al. "SIP: Session Initiation Protocol," Network Working Group, RFC 2543 and Internet Drafts (12/96-3/99). (Handley, RFC 2543)	
	D105	FreeS/WAN Project, *Linux FreeS/WAN Compatibility Guide* (March 4, 1999). (FreeS/WAN Compatibility Guide, FreeS/WAN)	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

	D106	Telcordia Technologies, "ANX Release 1 Document Corrections," AIAG (May 11, 1999). (Telcordia, ANX)	
	D107	Ken Hornstein & Jeffrey Altman, *Distributing Kerberos KDC and Realm Information with DNS* <draft-eitf-cat-krb-dns-locate-oo.txt> (June 21, 1999). (Hornstein, DNS SRV)	
	D108	Bhattacharya, et al., "An LDAP Schema for Configuration and Administration of IPSec Based Virtual Private Networks (VPNs)", IETF Internet Draft (October 1999). (Bhattcharya LDAP VPN)	
	D109	B. Patel, et al. "DHCP Configuration of IPSEC Tunnel Mode," IPSEC Working Group, Internet Draft 02 (10/15/1999). (Patel)	
	D110	Goncalves, et al. *Check Point FireWall-1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW)	
	D111	"Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources," FirstVPN, (Jan 2000). (FirstVPN Microsoft)	
	D112	Gulbrandsen, Vixie, & Esibov, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2782 (February 2000). (RFC 2782, DNS SRV)	
	D113	MITRE Organization, "Technical Description," Collaborative Operations in Joint Expeditionary Force Experiment (JEFX) 99 (February 2000). (MITRE, SIPRNET)	
	D114	H. Schulzrinne, et al. "Application-Layer Mobility Using SIP," Mobile Computing and Communications Review, Vol. 4, No. 3. pp. 47-57 (July 2000). (Application, SIP)	
	D115	Kindred et al, "Dynamic VPN Communities: Implementation and Experience," DARPA Information Survivability Conference and Exposition II (June 2001). (DARPA, VPN SYSTEMS)	
	D116	ANX 101: Basic ANX Service Outline. (Outline, ANX)	
	D117	ANX 201: Advanced ANX Service. (Advanced, ANX)	
	D118	Appendix A: Certificate Profile for ANX IPsec Certificates. (Appendix, ANX)	
	D119	Assured Digital Products. (Assured Digital)	
	D120	Aventail Corp., "Aventail AutoSOCKS the Client Key to Network Security," Aventail Corporation White Paper. (Network Security, Aventail)	
	D121	Cindy Moran, "DISN Data Networks: Secret Internet Protocol Router Network (SIPRNet)." (Moran, SIPRNET)	
	D122	Data Fellows F-Secure VPN+ (F-Secure VPN+)	
	D123	"Interim Operational Systems Doctrine for the Remote Access Security Program (RASP) Secret Dial-In Solution. (RASP, SIPRNET)	
	D124	*Onion Routing*, "Investigation of Route Selection Algorithms," *available at* http://www.onion-router.net/Archives/Route/index.html. (Route Selection, Onion Routing)	
	D125	Secure Computing, "Bullet-Proofing an Army Net," Washington Technology. (Secure, SIPRNET)	
	D126	SPARTA "Dynamic Virtual Private Network." (Sparta, VPN SYSTEMS)	
	D127	Standard Operation Procedure for Using the 1910 Secure Modems. (Standard, SIPRNET)	
	D128	Publically available emails relating to FreeS/WAN (MSFTVX00018833-MSFTVX00019206). (FreeS/WAN emails, FreeS/WAN)	
	D129	Kaufman et al., "Implementing IPsec," (Copyright 1999) (Implementing IPsec)	
	D130	Network Associates *Gauntlet Firewall For Unix User's Guide Version 5.0* (1999). (Gauntlet User's Guide – Unix, Firewall Products)	
	D131	Network Associates *Gauntlet Firewall For Windows NT Getting Started Guide Version 5.0* (1999) (Gauntlet Getting Started Guide – NT, Firewall Products)	
	D132	Network Associates *Gauntlet Firewall For Unix Getting Started Guide Version 5.0* (1999) (Gauntlet Unix Getting Started Guide, Firewall Products)	
	D133	Network Associates *Release Notes Gauntlet Firewall for Unix 5.0* (March 19, 1999) (Gauntlet Unix Release Notes, Firewall Products)	
	D134	Network Associates *Gauntlet Firewall For Windows NT Administrator's Guide Version 5.0* (1999) (Gauntlet NT Administrator's Guide, Firewall Products)	
	D135	Trusted Information Systems, Inc. *Gauntlet Internet Firewall Firewall-to-Firewall Encryption Guide Version 3.1* (1996) (Gauntlet Firewall-to-Firewall, Firewall Products)	
	D136	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	D137	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	D138	Dan Sterne *Dynamic Virtual Private Networks* (May 23, 2000) (Sterne DVPN, DVPN)	
	D139	Darrell Kindred *Dynamic Virtual Private Networks (DVPN)* (December 21, 1999) (Kindred DVPN, DVPN)	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

	D140	Dan Sterne *et al. TIS Dynamic Security Perimeter Research Project Demonstration* (March 9, 1998) (Dynamic Security Perimeter, DVPN)	
	D141	Darrell Kindred *Dynamic Virtual Private Networks Capability Description* (January 5, 2000) (Kindred DVPN Capability, DVPN) 11	
	D142	October 7, and 28 1997 email from Domenic J. Turchi Jr. (SPARTA00001712-1714, 1808-1811) (Turchi DVPN email, DVPN)	
	D143	James Just & Dan Sterne *Security Quickstart Task Update* (February 5, 1997) (Security Quickstart, DVPN)	
	D144	Virtual Private Network Demonstration dated March 21, 1998 (SPARTA00001844-54) (DVPN Demonstration, DVPN)	
	D145	GTE Internetworking & BBN Technologies DARPA *Information Assurance Program Integrated Feasibilit Demonstration (IFD) 1.1 Plan* (March 10, 1998) (IFD 1.1, DVPN)	
	D146	Microsoft Corp. Windows NT Server Product Documentation: Administration Guide - Connection Point Services, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cpsops.mspx (Connection Point Services) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D147	Microsoft Corp. Windows NT Server Product Documentation: Administration Kit Guide - Connection Manager, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cmak.mspx (Connection Manager) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D148	Microsoft Corp. Autodial Heuristics, *available at* http://support.microsoft.com/kb/164249 (Autodial Heuristics) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D149	Microsoft Corp., Cariplo: Distributed Component Object Model, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms809332(printer).aspx (Cariplo I)	
	D150	Marc Levy, COM Internet Services (Apr. 23, 1999), *available at* http://msdn2.microsoft.com/en-us/library/ms809302(printer).aspx (Levy)	
	D151	Markus Horstmann and Mary Kirtland, DCOM Architecture (July 23, 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809311(printer).aspx (Horstmann)	
	D152	Microsoft Corp., DCOM: A Business Overview (Apr. 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809320(printer).aspx (DCOM Business Overview I)	
	D153	Microsoft Corp., DCOM Technical Overview (Nov. 1996), *available at* http://msdn2.microsoft.com/en-us/library/ms809340(printer).aspx (DCOM Technical Overview I)	
	D154	Microsoft Corp., DCOM Architecture White Paper (1998) *available in* PDC DVD-ROM (DCOM Architecture)	
	D155	Microsoft Corp, DCOM – The Distributed Component Object Model, A Business Overview White Paper (Microsoft 1997) *available in* PDC DVD-ROM (DCOM Business Overview II)	
	D156	Microsoft Corp., DCOM - Cariplo Home Banking Over The Internet White Paper Microsoft 1996) *available in* PDC DVD-ROM (Cariplo II)	
	D157	Microsoft Corp., DCOM Solutions in Action White Paper (Microsoft 1996) *available in* PDC DVD-ROM (DCOM Solutions in Action)	
	D158	Microsoft Corp., DCOM Technical Overview White Paper (Microsoft 1996) *available* 12 *in* PDC DVD-ROM (DCOM Technical Overview II)	
	D159	125. Scott Suhy & Glenn Wood, DNS and Microsoft Windows NT 4.0, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms810277(printer).aspx (Suhy)	
	D160	126. Aaron Skonnard, *Essential WinInet* 313-423 (Addison Wesley Longman 1998) (Essential WinInet)	
	D161	Microsoft Corp. Installing, Configuring, and Using PPTP with Microsoft Clients and Servers, (1998) *available at* http://msdn2.microsoft.com/enus/library/ms811078(printer).aspx (Using PPTP)	
	D162	Microsoft Corp., Internet Connection Services for MS RAS, Standard Edition, http://www.microsoft.com/techneUarchive/winntas/proddocs/inetconctservice/bcgstart.mspx (Internet Connection Services I)	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

	D163	Microsoft Corp., Internet Connection Services for RAS, Commercial Edition, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstrtc.mspx (Internet Connection Services II)	
	D164	Microsoft Corp., Internet Explorer 5 Corporate Deployment Guide – Appendix B: Enabling Connections with the Connection Manager Administration Kit, *available at* http://www.microsoft.com/technet/prodtechnol/ie/deploy/deploy5/appendb.mspx (IE5 Corporate Development)	
	D165	Mark Minasi, *Mastering Windows NT Server 4* 1359-1442 (6th ed., January 15, 1999) (Mastering Windows NT Server)	
	D166	*Hands On, Self-Paced Training for Supporting Version 4.0* 371-473 (Microsoft Press 1998) (Hands On)	
	D167	Microsoft Corp., MS Point-to-Point Tunneling Protocol (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/maintain/featusability/pptpwp3.mspx (MS PPTP)	
	D168	Kenneth Gregg, *et al., Microsoft Windows NT Server Administrator's Bible* 173-206, 883-911, 974-1076 (IDG Books Worldwide 1999) (Gregg)	
	D169	Microsoft Corp., Remote Access (Windows), *available at* http://msdn2.microsoft.com/enus/library/bb545687(VS.85.printer).aspx (Remote Access)	
	D170	Microsoft Corp., Understanding PPTP (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/plan/pptpudst.mspx (Understanding PPTP NT 4) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D171	Microsoft Corp., Windows NT 4.0: Virtual Private Networking, *available at* http://www.microsoft.com/technet/archive/winntas/deploy/confeat/vpntwk.mspx (NT4 VPN) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D172	Anthony Northrup, *NT Network Plumbing: Routers, Proxies, and Web Services* 299-399 (IDG Books Worldwide 1998) (Network Plumbing)	
	D173	Microsoft Corp., Chapter 1 - Introduction to Windows NT Routing with Routing and Remote Access Service, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/rras40/rrasch0l.mspx (Intro to RRAS) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.) 13	
	D174	Microsoft Corp., Windows NT Server Product Documentation: Chapter 5 - Planning for Large-Scale Configurations, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/rras40/rrasch05.mspx (Large-Scale Configurations) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D175	F-Secure, *F-Secure NameSurfer*(May 1999) (from FSECURE 00000003) (NameSurfer 3)	
	D176	F-Secure, *F-Secure VPN Administrator's Guide* (May 1999) (from FSECURE 00000003) F-Secure VPN 3)	
	D177	F-Secure, *F-Secure SSH User's & Administrator's Guide* (May 1999) (from FSECURE 00000003) (SSH Guide 3)	
	D178	F-Secure, *F-Secure SSH2.0 for Windows NT and 95* (May 1999) (from FSECURE 00000003) (SSH 2.0 Guide 3)	
	D179	F-Secure, *F-Secure VPN+ Administrator's Guide* (May 1999) (from FSECURE 00000003) (VPN+ Guide 3)	
	D180	F-Secure, *F-Secure VPN+ 4.1* (1999) (from FSECURE 00000006) (VPN+ 4.1 Guide 6)	
	D181	F-Secure, *F-Secure SSH* (1996) (from FSECURE 00000006) (F-Secure SSH 6)	
	D182	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (1998) (from FSECURE 00000006) (F-Secure SSH 2.0 Guide 6)	
	D183	F-Secure, *F-Secure SSH User's & Administrator's Guide* (Sept. 1998) (from FSECURE 00000009) (SSH Guide 9)	
	D184	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (Sept. 1998) (from FSECURE 00000009) (F-Secure SSH 2.0 Guide 9)	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

	D185	F-Secure, *F-Secure VPN+* (Sept. 1998) (from FSECURE 00000009) (VPN+ Guide 9)	
	D186	F-Secure, *F-Secure Management Tools, Administrator's Guide* (1999) (from FSECURE 00000003) (F-Secure Management Tools)	
	D187	F-Secure, *F-Secure Desktop, User's Guide* (1997) (from FSECURE 00000009) (FSecure Desktop User's Guide)	
	D188	SafeNet, Inc., *VPN Policy Manager* (January 2000) (VPN Policy Manager)	
	D189	F-Secure, *F-Secure VPN+ for Windows NT 4.0* (1998) (from FSECURE 00000009) (FSecure VPN+)	
	D190	IRE, Inc., *SafeNet/Security Center Technical Reference Addendum* (June 22, 1999) (Safenet Addendum)	
	D191	IRE, Inc., *System Description for VPN Policy Manager and SafeNet/SoftPK* (March 30, 2000) (VPN Policy Manager System Description)	
	D192	IRE, Inc., *About SafeNet / VPN Policy Manager* (1999) (About Safenet VPN Policy Manager)	
	D193	Trusted Information Systems, Inc., *Gauntlet Internet Firewall, Firewall Product Functional Summary* July 22, 1996) (Gauntlet Functional Summary)	
	D194	Trusted Information Systems, Inc., *Running the Gauntlet Internet Firewall, An Administrator's Guide to Gauntlet Version 3.0* (May 31, 1995) (Running the Gauntlet Internet Firewall)	
	D195	Ted Harwood, *Windows NT Terminal Server and Citrix Metaframe* (New Riders 1999) (Windows NT Harwood) 79	
	D196	Todd W. Mathers and Shawn P. Genoway, *Windows NT Thing Client Solutions: Implementing Terminal Server and Citrix MetaFrame* (Macmillan Technical Publishing 1999) (Windows NT Mathers)	
	D197	Bernard Aboba et al., *Securing L2TP using IPSEC* (February 2, 1999)	
	D198	156. *Finding Your Way Through the VPN Maze* (1999) ("PGP")	
	D199	Linux FreeS/WAN Overview (1999) (Linux FreeS/WAN Overview)	
	D200	TimeStep, *The Business Case for Secure VPNs* (1998) ("TimeStep")	
	D201	WatchGuard Technologies, Inc., *WatchGuard LiveSecurity for MSS Powerpoint* (Feb. 14 2000)	
	D202	WatchGuard Technologies, Inc., *MSS Version 2.5, Add-On for WatchGuard SOHO Releaset Notes* (July 21, 2000)	
	D203	WatchGuard Technologies, Inc., *MSS Firewall Specifications* (1999)	
	D204	WatchGuard Technologies, Inc., *Request for Information, Security Services* (2000)	
	D205	WatchGuard Technologies, Inc., *Protecting the Internet Distributed Enterprise, White Paper* (February 2000)	
	D206	Air Force Research Laboratory, *Statement of Work for Information Assurance System Architecture and Integration, PR No. N-8-6106 (Contract No. F30602-98-C-0012)* (January 29, 1998)	
	D207	Technologies, Inc., *WatchGuard Firebox System Powerpoint* (2000)	
	D208	GTE Internetworking & BBN Technologies DARPA *Information Assurance Program Integrated Feasibility Demonstration 1FD 1.2 Report, Rev. 1.0* (September 21, 1998)	
	D209	BBN Information Assurance Contract, *TIS Labs Monthly Status Report* (March 16-April 30, 1998)	
	D210	DARPA, *Dynamic Virtual Private Network (VPN) Powerpoint*	
	D211	GTE Internetworking, *Contractor's Program Progress Report* (March 16-April 30, 1998)	
	D212	Darrell Kindred, *Dynamic Virtual Private Networks (DVPN) Countermeasure Characterization* (January 30, 2001)	
	D213	*Virtual Private Networking Countermeasure Characterization* (March 30, 2000)	
	D214	*Virtual Private Network Demonstration* (March 21, 1998)	
	D215	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks (VPNs) and Integrated Security Management* (2000)	
	D216	Information Assurance/NAI Labs, *Create/Add DVPN Enclave* (2000)	
	D217	NAI Labs, *IFE 3.1 Integration Demo* (2000)	
	D218	Information Assurance, *Science Fair Agenda* (2000)	
	D219	Darrell Kindred et al., *Proposed Threads for IFE 3.1* (January 13, 2000)	
	D220	*IFE 3.1 Technology Dependencies* (2000)	
	D221	*IFE 3.1 Topology* (February 9, 2000)	
	D222	Information Assurance, *Information Assurance Integration: IFE 3.1, Hypothesis & Thread Development* January 10-11, 2000)	
	D223	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation* (2000)	
	D224	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.2* (2000)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D225	Information Assurance/NAI Labs, Dynamic Virtual Private Networks Presentation v.3 (2000)	
	D226	T. Braun et al., *Virtual Private Network Architecture*, Charging and Accounting Technology for the Internet (August 1, 1999) (VPNA)	
	D227	Network Associates Products - *PGP Total Network Security Suite, Dynamic Virtual Private Networks* (1999)	
	D228	Microsoft Corporation, *Microsoft Proxy Server 2.0* (1997) (Proxy Server 2.0, Microsoft Prior Art VPN Technology)	
	D229	David Johnson et. al., *A Guide To Microsoft Proxy Server 2.0* (1999) (Johnson, Microsoft Prior Art VPN Technology)	
	D230	Microsoft Corporation, *Setting Server Parameters* (1997 (copied from Proxy Server 2.0 CD labeled MSFTVX00157288) (Setting Server Parameters, Microsoft Prior Art VPN Technology)	
	D231	Kevin Schuler, *Microsoft Proxy Server 2* (1998) (Schuler, Microsoft Prior Art VPN Technology)	
	D232	Erik Rozell et. al., *MCSE Proxy Server 2 Study Guide* (1998) (Rozell, Microsoft Prior 15 Art VPN Technology)	
	D233	M. Shane Stigler & Mark A Linsenbardt, *IIS 4 and Proxy Server 2* (1999) (Stigler, Microsoft Prior Art VPN Technology)	
	D234	David G. Schaer, *MCSE Test Success: Proxy Server 2*(1998) (Schaer, Microsoft Prior Art VPN Technology)	
	D235	John Savill, *The Windows NT and Windows 2000 Answer Book* (1999) (Savill, Microsoft Prior Art VPN Technology)	
	D236	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	D237	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	D238	File History for U.S. Application Serial No. 09/653,201, Applicant(s): Whittle Bryan, et al., Filing Date 08/31/2000.	
	D239	*AutoSOCKS v2. 1*, Datasheet, http://web.archive.org/web/19970212013409/www.aventail.com/prod/autoskds.html	
	D240	Ran Atkinson, *Use of DNS to Distribute Keys*, 7 Sept. 1993, http://ops.ietf.org/lists/namedroppers/namedroppers, 1 99x/msg00945.html	
	D241	FirstVPN Enterprise Networks, Overview	
	D242	Chapter 1: Introduction to Firewall Technology, Administration Guide; 12/19/07, http://www.books24x7.com/book/id_762/viewer_r.asp?bookid=762&chunked=41065062	
	D243	The TLS Protocol Version 1.0; January 1999; page 65 of 71.	
	D244	Elizabeth D. Zwicky, et al., Building Internet Firewalls, 2nd Ed.	
	D245	Virtual Private Networks - Assured Digital Incorporated - ADI 4500; http://web.archive.org/web/19990224050035/www.assured-digital.com/products/prodvpn/adia4500.htm	
	D246	Accessware - The Third Wave in Network Security, Conclave from Internet Dynamics; http://web.archive.org/web/11980210013830/interdyn.com/Accessware.html	
	D247	Extended System Press Release, Sept. 2, 1997; *Extended VPN Uses The Internet to Create Virtual Private Networks*, www.extendedsystems.com	
	D248	Socks Version 5; Executive Summary; http://web.archive.org/web/199970620031945/www.aventail.com/educate/whitepaper/sockswp.html	
	D249	Internet Dynamics First to Ship Integrated Security Solutions for Enterprise Intranets and Extranets; Sept. 15, 1997; http://web.archive.org/web/19980210014150/interdyn.com	
	D250	Emails from various individuals to Linux IPsec re: DNS-LDAP Splicing	
	D251	Fasbender, A., et al., Variable and Scalable Security: Protection of Location Information in Mobile IP, IEEE VTS, 46th, 1996, 5 pp.	
	D252	David Kosiur, "Building and Managing Virtual Private Networks" (1998)	
	D253	Request for Inter Partes Reexamination of Patent No. 6,502,135, dated Nov. 25, 2009.	
	D254	Request for Inter Partes Reexamination of Patent No. 7,188,180, dated Nov. 25, 2009.	
	D255	Yuan Dong Feng, "A novel scheme combining interleaving technique with cipher in Rayleigh fading channels," Proceedings of the International Conference on Communication technology, 2:S47-02-1-S47-02-4 (1998)	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

	D256	Davies and Price, edited by Tadahiro Uezono, "Network Security", Japan, Nikkei McGraw-Hill, December 5, 1958, First Edition, first copy, p. 102-108	
	D257	Davies et al., "An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer," Security for Computer Networks, Second Edition, pp. 98-101 (1989)	
	D258	Baumgartner et al, "Differentiated Services: A New Approach for Quality of Service in the Internet," International Conference on High Performance Networking, 255-273 (1998)	
	D259	Chapman et al., "Domain Name System (DNS)," 278-296 (1995)	
	D260	Davila et al., "Implementation of Virtual Private Networks at the Transport Layer," M. Mambo, Y. Zheng (Eds), Information Security (Second International) Workshop, ISW' 99. Lecture Notes in Computer Science (LNCS), Vol. 1729; 85-102 (1999)	
	D261	De Raadt et al., "Cryptography in OpenBSD," 10 pages (1999)	
	D262	Eastlake, "Domain Name System Security Extensions," Internet Citation, Retrieved from the Internet: URL:ftp://ftp.inet.no/pub/ietf/internet-drafts/draft-ietf-dnssec-secext2-05.txt (1998)	
	D263	Gunter et al., "An Architecture for Managing QoS-Enabled VRNs Over the Internet," Proceedings 24th Conference on Local Computer Networks. LCN' 99 IEEE Comput. Soc Los Alamitos, CA, pages 122-131 (1999)	
	D264	Shimizu, "Special Feature: Mastering the Internet with Windows 2000", Internet Magazine, 63:296-307 (2000)	
	D265	Stallings, "Cryptography and Network Security," Principals and Practice, 2nd Edition, pages 399-440 (1999)	
	D266	Takata, "U.S. Vendors Take Serious Action to Act Against Crackers – A Tracking Tool and a Highly Safe DNS Software are Released", Nikkei Communications, 257:87(1997)	
	D267	Wells, Email (Lancasterb1be@mail.msn.com), Subject: "Security Icon," (1998)	
	D268	Microsoft Corporation's Fifth Amended Invalidity Contentions dated September 18, 2009, VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation and invalidity claim charts for U.S. Patent Nos. 7,188,180 and 6,839,759	
	D269	The IPSEC Protocol as described in Atkinson, et al., "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998) ("RFC 2401"); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D270	S. Kent and R. Atkinson, "IP Authentication Header," RFC 2402 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D271	C. Madson and R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH," RFC 2403 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D272	C. Madson and R. Glenn, "The Use HMAC-SHA-1-96 within ESP and AH," RFC 2404 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D273	C. Madson and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV", RFC 2405 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D274	S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," RFC 2406 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D275	Derrell Piper, "The Internet IP Security Domain of Interpretation for ISAKMP," RFC 2407 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D276	Douglas Maughan, et al, "Internet Security Association and Key Management Protocol (ISAKMP)," RFC 2408 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D277	D. Harkins and D. Carrell, "The Internet Key Exchange (IKE)," RFC 2409 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D278	R. Glenn and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec." RFC 2410 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D279	R. Thayer, et al., "IP Security Document Roadmap," RFC 2411 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D280	Hilarie K. Orman, "The OAKLEY Key Determination Protocol," RFC 2412 (November 1998) in combination with J.M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose California (July 1996) ("Galvin")	
	D281	DNS-related correspondence dated September 7, 1993 to September 20, 1993. (Pre KX, KX Records)	
	D282	Aventail Corp., "AutoSOCKS v. 2.1 Datasheet," *available at* http://www.archive.org/web/19970212013409/www.aventail.com/prod/autosk2ds.html (1997). (AutoSOCKS, Aventail)	
	D283	Aventail Corp., "Socks Version 5," Aventail Whitepaper, *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/soc kswp.html (1997). (Socks, Aventail)	
	D284	Goncalves, et al. *Check Point FireWall -1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW)	
	D285	Assured Digital Products. (Assured Digital)	
	D286	F-Secure, *F-Secure Evaluation Kit* (May 1999) (FSECURE 00000003) (Evaluation Kit 3)	
	D287	F-Secure, *F-Secure Evaluation Kit* (Sept. 1998) (FSECURE 00000009) (Evaluation Kit 9)	
	D288	IRE, Inc., *SafeNet/Soft-PK Version 4* (March 28, 2000) (Soft-PK Version 4)	
	D289	IRE/SafeNet Inc., *VPN Technologies Overview* (March 28, 2000) (Safenet VPN Overview)	
	D290	IRE, Inc., *SafeNet/VPN Policy Manager Quick Start Guide Version 1* (1999) (SafeNet VPN Policy Manager)	
	D291	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.3* (2000)	
	D292	PCT International Search Report for related PCT Application No.: PCT/US01/13261, 8 pages .	
	D293	PCT International Search Report for related PCT Application No.: PCT/US99/25323, 3 pages .	
	D294	PCT International Search Report for related PCT Application No.: PCT/US99/25325, 3 pages .	
	D295	Deposition Transcript for Gary Tomlinson dated February 27, 2009	
	D296	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 8, 2010, 8:45 AM	
	D297	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 8, 2010, 1:30 PM	
	D298	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 9, 2010, 9:00 AM	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D299	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 9, 2010, 1:30 PM	
	D300	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 10, 2010, 9:00 AM	
	D301	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 10, 2010, 1:00 PM	
	D302	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 11, 2010, 9:00 AM	
	D303	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 11, 2010, 1:30 PM	
	D304	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 12, 2010, 9:00 AM	
	D305	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 12, 2010, 1:15 PM	
	D306	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 15, 2010, 9:00 AM	
	D307	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 15, 2010, 12:35 PM	
	D308	European Search Report dated January 24, 2011 from corresponding European Application Number 10011949.4	
	D309	European Search Report dated March 17, 2011 from corresponding European Application Number 10184502.2	
	D310	Hollenbeck et al., "Registry Registrar Protocol (RRP) Version 1.1.0; Internet Engineering Task Force, 34 pages (1999)	
	D311	Tannenbaum, "Computer Networks," pages 202-219 (1996)	
	D312	Defendants' Preliminary Joint Invalidity Contentions dated July 1, 2011	
	D313	Appendix B: DNS References to Defendants' Preliminary Joint Invalidity Contentions dated July 1, 2011	
	D314	Appendix A to Defendants' Preliminary Joint Invalidity Contentions dated July 1, 2011	
	D315	Exhibit 1, IETF RFC 2065: Domain Name System Security Extensions; Published January 1997[1] vs. Claims of the '211 Patent[2]	
	D316	Exhibit 2, IETF RFC 2065: Domain Name System Security Extensions; Published January 1997[1] vs. Claims of the '504 Patent[2]	
	D317	Exhibit 3, RFC 2543[1] vs. Claims of the '135 Patent[2]	
	D318	Exhibit 4, RFC 2543[1] vs. Claims of the '211 Patent[2]	
	D319	Exhibit 5, RFC 2543[1] vs. Claims of the '504 Patent[2]	
	D320	Exhibit 6, SIP Draft v.2[1] vs. Claims of the '135 Patent[2]	
	D321	Exhibit 7, SIP Draft v.2[1] vs. Claims of the '211 Patent[2]	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D322	Exhibit 8, SIP Draft v.2[1] vs. Claims of the '504 Patent[2]	
	D323	Exhibit 9, H.323[1] vs. Claims of the '135 Patent[2]	
	D324	Exhibit 10, H.323[1] vs. Claims of the '211 Patent[2]	
	D325	Exhibit 11, H.323[1] vs. Claims of the '504 Patent[2]	
	D326	Exhibit 12, SSL 3.0[1] vs. Claims of the '135 Patent[2].	
	D327	Exhibit 13, SSL 3.0[1] vs. Claims of the '211 Patent[2]	
	D328	Exhibit 14, SSL 3.0[1] vs. Claims of the '504 Patent[2]	
	D329	Exhibit 15, RFC 2487[1] vs. Claims of the '135 Patent[2]	
	D330	Exhibit 16, RFC 2487[1] vs. Claims of the '211 Patent[2]	
	D331	Exhibit 17, RFC 2487[1] vs. Claims of the '504 Patent[2]	
	D332	Exhibit 18, RFC 2595[1] vs. Claims of the '135 Patent[2]	
	D333	Exhibit 19, RFC 2595[1] vs. Claims of the '211 Patent[2]	
	D334	Exhibit 20, RFC 2595[1] vs. Claims of the '504 Patent[2]	
	D335	Exhibit 21, iPass[1] vs. Claims of the '135 Patent[2]	
	D336	Exhibit 22, iPASS[1] vs. Claims of the '211 Patent[2]	
	D337	Exhibit 23, iPASS[1] vs. Claims of the '504 Patent[2]	
	D338	Exhibit 24, "US '034"[1] vs. Claims of the '135 Patent[2]	
	D339	Exhibit 25, US Patent No. 6,453,034 ("US '034")[1] vs. Claims of the '211 Patent[2]	
	D340	Exhibit 26, US Patent No. 6,453,034 ("US '034")[1] vs. Claims of the '504 Patent[2]	
	D341	Exhibit 27, US '287[1] vs. Claims of the '135 Patent[2]	
	D342	Exhibit 28, US '287[1] vs. Claims of the '211 Patent[2]	
	D343	Exhibit 29, US '287[1] vs. Claims of the '504 Patent[2]	
	D344	Exhibit 30, Overview of Access VPNs[1] vs. Claims of the '135 Patent[2]	
	D345	Exhibit 31, Overview of Access VPNs[1] vs. Claims of the '211 Patent[2]	
	D346	Exhibit 32, Overview of Access VPNs[1] vs. Claims of the '504 Patent[2]	
	D347	Exhibit 34, RFC 1928[1] vs. Claims of the '135 Patent[2]	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D348	Exhibit 35, RFC 1928[1] vs. Claims of the '211 Patent[2]	
	D349	Exhibit 36, RFC 1928[1] vs. Claims of the '504 Patent[2]	
	D350	Exhibit 37, RFC 2661[1] vs. Claims of the '135 Patent[2]	
	D351	Exhibit 38, RFC 2661[1] vs. Claims of the '211 Patent[2]	
	D352	Exhibit 39, RFC 2661[1] vs. Claims of the '504 Patent[2]	
	D353	Exhibit 40, SecureConnect[1] vs. Claims of the '135 Patent[2]	
	D354	Exhibit 41, SecureConnect[1] vs. Claims of the '211 Patent[2]	
	D355	Exhibit 42,SecureConnect[1] vs. Claims of the '504 Patent[2]	
	D356	Exhibit 43, SFS-HTTP[1] vs. Claims of the '135 Patent[2]	
	D357	Exhibit 44, SFS-HTTP[1] vs. Claims of the '211 Patent[2]	
	D358	Exhibit 45, SFS-HTTP[1] vs. Claims of the '504 Patent[2]	
	D359	Exhibit 46, US '883[1] vs. Claims of the '135 Patent[2]	
	D360	Exhibit 47, US '883[1] vs. Claims of the '211 Patent[2]	
	D361	Exhibit 48, US '883[1] vs. Claims of the '504 Patent[2]	
	D362	Exhibit 49, US '132[1] vs. Claims of the '135 Patent[2]	
	D363	Exhibit 50, US '132[1] vs. Claims of the '211 Patent[2]	
	D364	Exhibit 51, US '132[1] vs. Claims of the '504 Patent[2]	
	D365	Exhibit 52, US '213[1] vs. Claims of the '135 Patent[2]	
	D366	Exhibit 53, US '213[1] vs. Claims of the '211 Patent[2]	
	D367	Exhibit 54, US '213[1] vs. Claims of the '504 Patent[2]	
	D368	Exhibit 55, B&M VPNs[1] vs. Claims of the '135 Patent[2]	
	D369	Exhibit 56, B&M VPNs[1] vs. Claims of the '211 Patent[2]	
	D370	Exhibit 57, B&M VPNs[1] vs. Claims of the '504 Patent[2]	
	D371	Exhibit 58, BorderManager[1] vs. Claims of the '135 Patent[2]	
	D372	Exhibit 59, BorderManager[1] vs. Claims of the '211 Patent[2]	
	D373	Exhibit 60, BorderManager[1] vs. Claims of the '504 Patent[2]	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D374	Exhibit 61, Prestige 128 Plus[1] vs. Claims of the '135 Patent[2]	
	D375	Exhibit 62, Prestige 128 Plus[1] vs. Claims of the '211 Patent[2]	
	D376	Exhibit 63, Prestige 128 Plus[1] vs. Claims of the '504 Patent[2]	
	D377	Exhibit 64, RFC 2401[1] vs. Claims of the '135 Patent[2]	
	D378	Exhibit 65, RFC 2401[1] vs. Claims of the '211 Patent[2]	
	D379	Exhibit 66, RFC 2401[1] vs. Claims of the '504 Patent[2]	
	D380	Exhibit 67, RFC 2486[1] vs. Claims of the '135 Patent[2]	
	D381	Exhibit 68, RFC 2486[1] vs. Claims of the '211 Patent[2]	
	D382	Exhibit 69, RFC 2486[1] vs. Claims of the '504 Patent[2]	
	D383	Exhibit 70, Understanding IPSec[1] vs. Claims of the '135 Patent[2]	
	D384	Exhibit 71, Understanding IPSec[1] vs. Claims of the '211 Patent[2]	
	D385	Exhibit 72, Understanding IPSec[1] vs. Claims of the '504 Patent[2]	
	D386	Exhibit 73, US '820[1] vs. Claims of the '135 Patent[2]	
	D387	Exhibit 74, US '820[1] vs. Claims of the '211 Patent[2]	
	D388	Exhibit 75, US '820[1] vs. Claims of the '504 Patent[2]	
	D389	Exhibit 76, US '019[1] vs. Claims of the '211 Patent[2]	
	D390	Exhibit 77, US '019[1] vs. Claims of the '504 Patent[2]	
	D391	Exhibit 78, US '049[1] vs. Claims of the '135 Patent[2]	
	D392	Exhibit 79, US '049[1] vs. Claims of the '211 Patent[2]	
	D393	Exhibit 80, US '049[1] vs. Claims of the '504 Patent[2]	
	D394	Exhibit 81, US '748[1] vs. Claims of the '135 Patent[2]	
	D395	Exhibit 82, US '261[1] vs. Claims of the '135 Patent[2]	
	D396	Exhibit 83, US '261[1] vs. Claims of the '211 Patent[2]	
	D397	Exhibit 84, US '261[1] vs. Claims of the '504 Patent[2]	
	D398	Exhibit 85, US '900[1] vs. Claims of the '135 Patent[2]	
	D399	Exhibit 86, US '900[1] vs. Claims of the '211 Patent[2]	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D400	Exhibit 87, US '900[1] vs. Claims of the '504 Patent[2]	
	D401	Exhibit 88, US '671[1] vs. Claims of the '135 Patent[2]	
	D402	Exhibit 89, US '671[1] vs. Claims of the '211 Patent[2]	
	D403	Exhibit 90, US '671[1] vs. Claims of the '504 Patent[2]	
	D404	Exhibit 91, JP '704[1] vs. Claims of the '135 Patent[2]	
	D405	Exhibit 92, JP '704[1] vs. Claims of the '211 Patent[2]	
	D406	Exhibit 93, JP '704[1] vs. Claims of the '504 Patent[2]	
	D407	Exhibit 94, GB '841[1] vs. Claims of the '135 Patent[2]	
	D408	Exhibit 95, GB '841[1] vs. Claims of the '211 Patent[2]	
	D409	Exhibit 96, GB '841[1] vs. Claims of the '504 Patent[2]	
	D410	Exhibit 97, US '318[1] vs. Claims of the '135 Patent[2]	
	D411	Exhibit 98, US '318[1] vs. Claims of the '211 Patent[2]	
	D412	Exhibit 99, US '318[1] vs. Claims of the '504 Patent[2]	
	D413	Exhibit 100, VPN/VLAN[1] vs. Claims of the '135 Patent[2]	
	D414	Exhibit 101, Nikkei[1] vs. Claims of the '135 Patent[2]	
	D415	Exhibit 102, NIKKEI[1] vs. Claims of the '211 Patent[2]	
	D416	Exhibit 103, NIKKEI[1] vs. Claims of the '504 Patent[2]	
	D417	Exhibit 104, Special Anthology[1] vs. Claims of the '135 Patent[2]	
	D418	Exhibit 105, Omron[1] vs. Claims of the '135 Patent[2]	
	D419	Exhibit 106, Gauntlet System[1] vs. Claims of the '135 Patent[2]	
	D420	Exhibit 107, Gauntlet System[1] vs. Claims of the '151 Patent[2]	
	D421	Exhibit 108, Gauntlet System[1] vs. Claims of the '180 Patent[2]	
	D422	Exhibit 109, Gauntlet System[1] vs. Claims of the '211 Patent[2]	
	D423	Exhibit 110, Gauntlet System[1] vs. Claims of the '504 Patent[2]	
	D424	Exhibit 111, Gauntlet System[1] vs. Claims of the '759 Patent[2]	
	D425	Exhibit 112, IntraPort System[1] vs. Claims of the '135 Patent[2]	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D426	Exhibit 113, IntraPort System[1] vs. Claims of the '151 Patent[2]	
	D427	Exhibit 114, IntraPort System[1] vs. Claims of the '180 Patent[2]	
	D428	Exhibit 115, IntraPort System[1] vs. Claims of the '211 Patent[2]	
	D429	Exhibit 116, IntraPort System[1] vs. Claims of the '504 Patent[2]	
	D430	Exhibit 117, IntraPort System[1] vs. Claims of the '759 Patent[2]	
	D431	Exhibit 118, Altiga VPN System[1] vs. Claims of the '135 Patent[2]	
	D432	Exhibit 119, Altiga VPN System[1] vs. Claims of the '151 Patent[2]	
	D433	Exhibit 120, Altiga VPN System[1] vs. Claims of the '180 Patent[2]	
	D434	Exhibit 121, Altiga VPN System[1] vs. Claims of the '211 Patent[2]	
	D435	Exhibit 122, Altiga VPN System[1] vs. Claims of the '504 Patent[2]	
	D436	Exhibit 123, Altiga VPN System[1] vs. Claims of the '759 Patent[2]	
	D437	Exhibit 124, Kiuchi[1] vs. Claims of the '135 Patent[2]	
	D438	Exhibit 125, Kiuchi[1] vs. Claims of the '151 Patent[2]	
	D439	Exhibit 126, Kiuchi[1] vs. Claims of the '180 Patent[2]	
	D440	Exhibit 127, Kiuchi[1] vs. Claims of the '211 Patent[2]	
	D441	Exhibit 128, Kiuchi[1] vs. Claims of the '504 Patent[2]	
	D442	Exhibit 129, Kiuchi[1] vs. Claims of the '759 Patent[2]	
	D443	Exhibit 130, Overview of Access VPNs and Tunneling Technologies ("Overview")[1] vs. Claims of the '135 Patent[2]	
	D444	Exhibit 131, Overview of Access VPNs and Tunneling Technologies ("Overview")[1] vs. Claims of the '151 Patent[2]	
	D445	Exhibit 132, Overview of Access VPNs and Tunneling Technologies ("Overview")[1] vs. Claims of the '180 Patent[2]	
	D446	Exhibit 133, Overview of Access VPNs and Tunneling Technologies ("Overview")[1] vs. Claims of the '211 Patent[2]	
	D447	Exhibit 134, Overview of Access VPNs and Tunneling Technologies ("Overview")[1] vs. Claims of the '504 Patent[2]	
	D448	Exhibit 135, Overview[1] vs. Claims of the '759 Patent[2]	
	D449	Exhibit 136, RFC 2401[1] vs. Claims of the '759 Patent[2]	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D450	Exhibit 137, Schulzrinne[1] vs. Claims of the '135 Patent[2]	
	D451	Exhibit 138, Schulzrinne[1] vs. Claims of the '151 Patent[2]	
	D452	Exhibit 139, Schulzrinne[1] vs. Claims of the '180 Patent[2]	
	D453	Exhibit 140, Schulzrinne[1] vs. Claims of the '211 Patent[2]	
	D454	Exhibit 141, Schulzrinne[1] vs. Claims of the '504 Patent[2]	
	D455	Exhibit 142, Schulzrinne[1] vs. Claims of the '759 Patent[2]	
	D456	Exhibit 143, Solana[1] vs. Claims of the '135 Patent[2]	
	D457	Exhibit 144, Solana[1] vs. Claims of the '151 Patent[2]	
	D458	Exhibit 145, Solana[1] vs. Claims of the '180 Patent[2]	
	D459	Exhibit 146, Solana[1] vs. Claims of the '211 Patent[2]	
	D460	Exhibit 147, Solana[1] vs. Claims of the '504 Patent[2]	
	D461	Exhibit 148, Solana[1] vs. Claims of the '759 Patent[2]	
	D462	Exhibit 149, Atkinson[1] vs. Claims of the '135 Patent[2]	
	D463	Exhibit 150, Atkinson[1] vs. Claims of the '151 Patent[2]	
	D464	Exhibit 151, Atkinson[1] vs. Claims of the '180 Patent[2]	
	D465	Exhibit 152, Atkinson[1] vs. Claims of the '211 Patent[2]	
	D466	Exhibit 153, Atkinson[1] vs. Claims of the '504 Patent[2]	
	D467	Exhibit 154, Atkinson[1] vs. Claims of the '759 Patent[2]	
	D468	Exhibit 155, Marino[1] vs. Claims of the '135 Patent[2]	
	D469	Exhibit 156, Marino[1] vs. Claims of the '151 Patent[2]	
	D470	Exhibit 157, Marino[1] vs. Claims of the '180 Patent[2]	
	D471	Exhibit 158, Marino[1] vs. Claims of the '211 Patent[2]	
	D472	Exhibit 159, Marino[1] vs. Claims of the '504 Patent[2]	
	D473	Exhibit 160, Marino[1] vs. Claims of the '759 Patent[2]	
	D474	Exhibit 161, Aziz ('646)[1] vs. Claims of the '759 Patent[2]	
	D475	Exhibit 162, Wesinger[1] vs. Claims of the '135 Patent[2]	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

	D476	Exhibit 163, Wesinger[1] vs. Claims of the '151 Patent[2]	
	D477	Exhibit 164, Wesinger[1] vs. Claims of the '180 Patent[2]	
	D478	Exhibit 165, Wesinger[1] vs. Claims of the '211 Patent[2]	
	D479	Exhibit 166, Wesinger[1] vs. Claims of the '504 Patent[2]	
	D480	Exhibit 167, Wesinger[1] vs. Claims of the '759 Patent[2]	
	D481	Exhibit 168, Aziz ('234)[1] vs. Claims of the '135 Patent[2]	
	D482	Exhibit 169, Aziz ('234)[1] vs. Claims of the '151 Patent[2]	
	D483	Exhibit 170, Aziz ('234)[1] vs. Claims of the '180 Patent[2]	
	D484	Exhibit 171, Aziz ('234)[1] vs. Claims of the '211 Patent[2]	
	D485	Exhibit 172, Aziz ('234)[1] vs. Claims of the '504 Patent[2]	
	D486	Exhibit 173, Aziz ('234)[1] vs. Claims of the '759 Patent[2]	
	D487	Exhibit 174, Schneider[1] vs. Claims of the '759 Patent[2]	
	D488	Exhibit 175, Valencia[1] vs. Claims of the '135 Patent[2]	
	D489	Exhibit 176, Valencia[1] vs. Claims of the '151 Patent[2]	
	D490	Exhibit 177, Valencia[1] vs. Claims of the '180 Patent[2]	
	D491	Exhibit 178, Valencia[1] vs. Claims of the '211 Patent[2]	
	D492	Exhibit 179, Valencia[1] vs. Claims of the '504 Patent[2]	
	D493	Exhibit 180, RFC 2401 in Combination with U.S. Patent No. 6,496,867[1] vs. Claims of the '180 Patent[2]	
	D494	Exhibit 181, Davison[1] vs. Claims of the '135 Patent[2]	
	D495	Exhibit 182, Davison[1] vs. Claims of the '151 Patent[2]	
	D496	Exhibit 183, Davison[1] vs. Claims of the '180 Patent[2]	
	D497	Exhibit 184, Davison[1] vs. Claims of the '211 Patent[2]	
	D498	Exhibit 185, Davison[1] vs. Claims of the '504 Patent[2]	
	D499	Exhibit 186, Davison[1] vs. Claims of the '759 Patent[2]	
	D500	Exhibit 187, AutoSOCKS v2.1[1] vs. Claims of the '135 Patent[2]	
	D501	Exhibit 188, AutoSOCKS v2.1[1] vs. Claims of the '151 Patent[2]	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D502	Exhibit 189, AutoSOCKS v2.1 Administrator's Guide[1] vs. Claims of the '180 Patent[2]	
	D503	Exhibit 190, AutoSOCKS[1] vs. Claims of the '759 Patent[2]	
	D504	Exhibit 191, Aventail Connect 3.01/2.51[1] vs. Claims of the '135 Patent[2]	
	D505	Exhibit 192, Aventail Connect v3.01/2.51[1] vs. Claims of the '151 Patent[2]	
	D506	Exhibit 193, Aventail Connect 3.01/2.51[1] vs. Claims of the '180 Patent[2]	
	D507	Exhibit 194, Aventail Connect 3.01/2.51[1] vs. Claims of the '759 Patent[2]	
	D508	Exhibit 195, Aventail Connect 3.1/2.6 Administrator's Guide[1] vs. Claims of the '135 Patent[2]	
	D509	Exhibit 196, Aventail Connect 3.1/2.6 Administrator's Guide[1] vs. Claims of the '151 Patent[2]	
	D510	Exhibit 197, Aventail Connect 3.1/2.6[1] vs. Claims of the '180 Patent[2]	
	D511	Exhibit 198, Aventail Connect 3.1/2.6[1] vs. Claims of the '759 Patent[2]	
	D512	Exhibit 199, BinGO! User's User's Guide/Extended Features Reference[1] vs. Claims of the '151 Patent[2]	
	D513	Exhibit 200, BinGO! User's User's Guide/Extended Features Reference[1] vs. Claims of the '135 Patent[2]	
	D514	Exhibit 201, BinGO! vs. Claims of the '180 Patent[2]	
	D515	Exhibit 202, BinGO! vs. Claims of the '759 Patent[2]	
	D516	Exhibit 203, Broadband Forum Technical Report TR-025 (Issue 1.0/5.0)[1] vs. Claims of the '135 Patent[2]	
	D517	Exhibit 204, Domain Name System (DNS) Security[1] vs. Claims of the '211 Patent[2]	
	D518	Exhibit 205, Domain Name System (DNS) Security[1] vs. Claims of the '504 Patent[2]	
	D519	Exhibit 206, RFC 2230, Key Exchange Delegation Record for the DNS[1] vs. Claims of the '211 Patent[2]	
	D520	Exhibit 207, RFC 2230, Key Exchange Delegation Record for the DNS[1] vs. Claims of the '504 Patent[2]	
	D521	Exhibit 208, RFC 2538, Storing Certificates in the Domain Name System (DNS)[1] vs. Claims of the '211 Patent[2]	
	D522	Exhibit 209, RFC 2538, Storing Certificates in the Domain Name System (DNS)[1] vs. Claims of the '504 Patent[2]	
	D523	Exhibit 210, IETF RFC 2065: Domain Name System Security Extensions; Published January 1997[1] vs. Claims of the '504 Patent[2]	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D524	Exhibit 211, IETF RFC 2065: Domain Name System Security Extensions; Published January 1997[1] vs. Claims of the '211 Patent[2]	
	D525	Exhibit 212, RFC 2486, RFC 2661, RFC 2401, and Internet-Draft, "Secure Remote Access with L2TP"[1] vs. Claims of the '135 Patent[2]	
	D526	Exhibit 213, U.S. Patent No. 7,100,195 in Combination with RFC 2401 and U.S. Patent No. 6,496,867[1] vs. Claims of the '135 Patent[2]	
	D527	Exhibit 214, U.S. Patent No. 7,100,195 in Combination with RFC 2401 and U.S. Patent No. 6,496,867[1] vs. Claims of the '151 Patent[2]	
	D528	Exhibit 215, U.S. Patent No. 6,643,701[1] vs. Claims of the '135 Patent[2]	
	D529	Exhibit 216, U.S. Patent No. 6,643,701[1] vs. Claims of the '151 Patent[2]	
	D530	Exhibit 217, U.S. Patent No. 6,496,867 in Combination with RFC 2401[1] vs. Claims of the '151 Patent[2]	
	D531	Exhibit 218, U.S. Patent No. 6,496,867 in Combination with RFC 2401[1] vs. Claims of the '135 Patent[2]	
	D532	Exhibit 219, U.S. Patent No. 6,496,867[1] vs. Claims of the '211 Patent[2]	
	D533	Exhibit 220, U.S. Patent No. 6,496,867[1] vs. Claims of the '504 Patent[2]	
	D534	Exhibit 221, RFC 2486, RFC 2661, RFC 2401, and Internet-Draft, "Secure Remote Access with L2TP"[1] vs. Claims of the '151 Patent[2]	
	D535	Exhibit 222, U.S. Patent No. 6,557,037[1] vs. Claims of the '211 Patent[2]	
	D536	Exhibit 223, U.S. Patent No. 6,557,037[1] vs. Claims of the '504 Patent[2]	
	D537	Exhibit 224, RFC 2230, Key Exchange Delegation Record for the DNS[1] vs. Claims of the '135 Patent[2]	
	D538	Exhibit 225, RFC 2230, Key Exchange Delegation Record for the DNS[1] vs. Claims of the '151 Patent[2]	
	D539	Exhibit Cisco-1, Cisco's Prior Art Systems[1] vs. Claims of the '135 Patent	
	D540	Exhibit Cisco-2, Cisco's Prior Art Systems[1] vs. Claims of the '151 Patent	
	D541	Exhibit Cisco-3, Cisco's Prior Art Systems[1] vs. Claims of the '180 Patent	
	D542	Exhibit Cisco-4, Cisco's Prior Art Systems[1] vs. Claims of the '211 Patent	
	D543	Exhibit Cisco-5, Cisco's Prior Art Systems[1] vs. Claims of the '504 Patent	
	D544	Exhibit Cisco-6, Cisco's Prior Art Systems[1] vs. Claims of the '759 Patent	
	D545	Exhibit Cisco-7, Cisco's Prior Art PIX System[1] vs. Claims of the '759 Patent	

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

	D546	Exhibit A: Copy of U.S. Patent No. 6,502,135	
	D547	Exhibit A: Copy of U.S. Patent No. 7,490,151	
	D548	Exhibit B: Certificate of Service to Request For Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 6,502,135)	
	D549	Exhibit B: Certificate of Service to Request For Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 7,490,151)	
	D550	Exhibit B-1: File History of U.S. Patent 6,502,135	
	D551	Exhibit B-2: Reexamination Record No. 95/001,269	
	D552	Exhibit C1: Claim Chart – Aventail Connect v3.1 (Patent No. 6,502,135)	
	D553	Exhibit C2: Claim Chart Aventail Connect V3.01 (Patent No. 6,502,135)	
	D554	Exhibit C-1: Copy of U.S. Patent No. 7,010,604	
	D555	Exhibit C2: Claim Chart Aventail Autosocks (Patent No. 7,490,151)	
	D556	Exhibit C1: Claim Chart Aventail Connect v3.01 (Patent No. 7,490,151)	
	D557	Exhibit C-2: Provisional Application 60/106,261	
	D558	Exhibit C3: Claim Chart Aventail AutoSOCKS (Patent No. 6,502,135)	
	D559	Exhibit C3: Claim Chart BinGO (Patent No. 7,490,151)	
	D560	Exhibit C-3: Provisional Application 60/137,704	
	D561	Exhibit C4: Claim Chart Wang (Patent No. 6,502,135)	
	D562	Exhibit C4: Claim Chart Beser (Patent No. 7,490,151)	
	D563	Exhibit C5: Claim Chart Beser (Patent No. 6,502,135)	
	D564	Exhibit C5: Claim Chart Wang (Patent No. 7,490,151)	
	D565	Exhibit C6: Claim Chart BinGO (Patent No. 6,502,135)	
	D566	Exhibit D: Memorandum Opinion in *VimetX v. Microsoft.*	
	D567	Exhibit D-1: Takahiro Kiuchi and Shigekoto Kaihara, "C-HTTP – The Development of a Secure, Closed HPPT-Based Network on the Internet," Published in the Proceedings of SNDSS 1996.	
	D568	Exhibit D-10: D.E. Denning and G.M. Sacco, "Time-stamps in Key Distribution Protocols," Communications of the ACM, Vol. 24, N.8, pp. 533-536. August 1981.	
	D569	Exhibit D-11: C.I. Dalton and J.F. Griffin, "Applying Military Grade Security to the Internet," Proceedings of the 8th Joint European Networking Conference (JENC 8), (May 12-15 1997).	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D570	Exhibit D-12: Steven M. Bellovin and Michael Merritt, "Encrypted Key Exchange: Password-Based protocols Secure against Dictionary Attacks," 1992 IEEE Symposium on Security and Privacy (1992).	
	D571	Exhibit D-2: Copy of U.S. Pat. No. 5,898,830	
	D572	Exhibit D-3: Eduardo Solana and Jürgen Harms, "Flexible Internet Secure Transactions Based on Collaborative Domains,", Security Protocols Workshop 1997, pp. 37-51.	
	D573	Exhibit D-4: Copy of U.S. Pat. No. 6,119,234	
	D574	Exhibit D-5: Jeff Sedayao, "'Mosaic Will Kill My Network!' – Studying Network Traffic Patterns of Mosaic Use," in Electron. Proc. 2nd World Wide Web Conf.'94: Mosaic and the Web, Chicago, IL, Oct. 1994.	
	D575	Exhibit D-6: M. Luby Juels and R. Ostrovsky, "Security of Blind Digital Signatures," Crypto '97, LNCS 1294, pages 150-164, Springer-Verlag, Berlin, 1997.	
	D576	Exhibit D-8: David M. Martin, "A Framework for Local Anonymity in the Internet," Technical Report. Boston University, Boston, MA, USA (Feb 21, 1998).	
	D577	Exhibit D-9: Copy of U.S. Pat. No. 7,764,231	
	D578	Exhibit E-1: Claim Charts Applying Kiuchi and Other References to Claims of the '135 Patent.	
	D579	Exhibit E1: Declaration of Chris Hopen (Patent No. 6,502,135)	
	D580	Exhibit E1: Declaration of Chris Hopen (Patent No. 7,490,151)	
	D581	Exhibit E-2: Claim Charts Applying Wesinger and Other References to Claims of the '135 Patent.	
	D582	Exhibit E2: Declaration of Michael Fratto (Patent No. 6,502,135)	
	D583	Exhibit E2: Declaration of Michael Fratto (Patent No. 7,490,151)	
	D584	Exhibit E-3: Claim Charts Applying Solana and Other References to Claims of the '135 Patent.	
	D585	Exhibit E3: Declaration of James Chester (Patent No. 6,502,135)	
	D586	Exhibit E3: Declaration of James Chester (Patent No. 7,490,151)	
	D587	Exhibit E-4: Claim Charts Applying Aziz and Other References to Claims of the '135 Patent.	
	D588	Exhibit X1: Aventail Connect Administrator's Guide v3.1/v2.6., PP 1-20 (1996-1999)	
	D589	Exhibit X10: Copy of U.S. Patent No. 4,885,778	
	D590	Exhibit X11: Copy of U.S. Patent No. 6,615,357	
	D591	Exhibit X2: Aventail Connect Administrator's Guide v3.01/v2.51., PP 1-116 (1996-1999)	
	D592	Exhibit X3: Aventail AutoSOCKS Administration & User's Guide v2.1., PP 1-70 (1996-1999)	
	D593	Exhibit X4: Reed et al., "Proxies for Anonymous Routine," 12th Annuary Computer Security Applications Conference, San Diego, CA, December -9-13, pp 1-10 (1996).	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D594	Exhibit X5: Wang, The Broadband Forum Technical Report, "TR-025 – Core Network Architecture Recommendations for Access to Legacy Data Networks over ADSL," Issue 1.0; pp. 1-24 , v1.0 (1999).	
	D595	Exhibit X6: Copy of U.S. Patent No. 6,496,867	
	D596	Exhibit X7: BinGO! User's Guide Incorporating by Reference BinGO! Extended Feature Reference.	
	D597	Exhibit X7: Kent et al., "Security Architecture for the Internet Protocol, " Network Working Group Request for Comments (RFC) 2401, pp 1-70 (1998).	
	D598	Exhibit X8: Copy of U.S. Patent No. 6,182,141	
	D599	Exhibit X9: BinGO! User's Guide v1.6 (1999).	
	D600	Exhibit Y1: Aventail Extranet Server 3.0 Administrator's Guide.	
	D601	Exhibit Y10: Hanks, S., et al., RFC1701, "Generic Routing Encapsulation (GRE)," 1994, Is Accessbile at http://www.ietf.org/rfc/rfc1701.txt.	
	D602	Exhibit Y10: Socolofsky, T. et al., RFC 1180, "A TCP/IP Tutorial," January 1991.	
	D603	Exhibit Y11: Simpson, W., editor, RFC 1661, "The Point-to-Point Protocol (PPP)," July 1994.	
	D604	Exhibit Y11: Simpson, W., RFC1994, "PPP Challenge Handshake Authentication Protocol (CHAP)," 1996, http://www.ietf.org/rdc/rfc1994.txt.	
	D605	Exhibit Y12: Meyer, G., RFC 1968, "The PPP Encryption Control Protocol (ECP)," June 1996.	
	D606	Exhibit Y12: Perkins, D., RFC1171, "The Point-To-Point Protocol for the Transmission of Multi-Protocol Datagrams over Point-To-Point Links," 1990, Is Accessible at http://www.ietf.org/rfc/rfc1171.txt.	
	D607	Exhibit Y13: Kummert, H., RFC 2420, "The PPP Triple-DES Encryption Protocol (3DESE)," September, 1998.	
	D608	Exhibit Y14: Townsley, W.M., et al., RFC 2661, "Layer Two Tunneling Protocol 'L2TP'," August 1999.	
	D609	Exhibit Y15: Pall, G.S., RFC 2118, "Microsoft Point-To-Point Encryption (MPPE) Protocol," March 1997.	
	D610	Exhibit Y16: Gross, G., et al., RFC 2364, "PPP Over AAL5," July 1998.	
	D611	Exhibit Y17: Srisuresh, P., RFC 2663, "IP Network Address Translator (NAT) Terminology and Considerations," August 1999.	
	D612	Exhibit Y18: Heinanen, J., RFC 1483, "Multiprotocol Encapsulation over ATM Adaptation Layer 5," July 1993.	
	D613	Exhibit Y2: Goldschlag et al., "Hiding Routing Information" (1996).	
	D614	Exhibit Y3: Copy of U.S. Patent No. 5,950,519	
	D615	Exhibit Y4: Ferguson, P. and Huston, G., "What Is a VPN", The Internet Protocol Journal, Vol 1., No. 1 (June 1998 ("Ferguson").	
	D616	Exhibit Y5: Mockapetris, P., RFC 1034, "Domain Names – Concepts and Facilities," November 1987 ("RFC1034").	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D617	Exhibit Y6: Mockapetris, P., RFC 1035, "Domain Names – Implementation and Specification," November 1987 ("RFC1035").	
	D618	Exhibit Y8: Fielding, R., et al., RFC 2068, "Hypertext Transfer Protocol – HTTP/1.1," January 1997.	
	D619	Exhibit Y8: Woodburn, R.A., et al., RFC1241, "A Scheme for an Internet Encapsulation Protocol: Version 1," 1991.	
	D620	Exhibit Y9: Leech, M., et al., RFC 1928, "Socks Protocol Version 5," March 1996.	
	D621	Exhibit Y9: Sirnpson, W., RFC1853, "IP in IP Tunneling," 1995, Is Accessible at http://ww.ietf.org/rfc/rfc1583.txt.	
	D622	Form PTO/SB/42, Listing Each Patent and Printed Publication Relied Upon to Provide a Substantial New Question of Patentability (Patent No. 6,502,135)	
	D623	Form PTO/SB/42, Listing Each Patent and Printed Publication Relied Upon to Provide a Substantial New Question of Patentability (Patent No. 7,490,151)	
	D624	Request for Inter Partes Reexamination (Patent No. 6,502,135)	
	D625	Request for Inter Partes Reexamination Transmittal Form (PTO/SB/58) (Patent No. 6,502,135)	
	D626	Request for Inter Partes Reexamination Transmittal Form (PTO/SB/58) (Patent No. 7,490,151)	
	D627	Request for Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 6,502,135)	
	D628	Request for Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 7,490,151)	
	D629	Transmittal Letter (Patent No. 6,502,135)	
	D630	Transmittal Letter (Patent No. 7,490,151)	
	D631	Joint Claim Construction and Prehearing Statement	
	D632	Exhibit A: Agreed Upon Terms; P.R. 4-3 Joint Claims Construction and Prehearing Statement	
	D633	Exhibit B: Disputed Claim Terms; P.R. 4-3 Joint Claim Construction and Prehearing Statement	
	D634	Exhibit C; VirnetX's Proposed Construction of Claim Terms and Supporting Evidence	
	D635	Exhibit D; Defendants' Intrinsic and Extrinsic Support; P.R. 4-3 Joint Claim Construction and Prehearing Statement	
	D636	File History of U.S. Patent 6,839,759	
	D637	Exhibit B-4; VirnetX, Inc. v. Microsoft Corp., Case No. 6:07-cv-80, Microsoft's Motion for Partial Summary Judgment of Invalidity of U.S. Patent No. 6,839,759 (E.D. Tex. Dec. 18, 2009)	
	D638	Exhibit D-2; Kent et al., "Security Architecture for the Internet Protocol," Internet Engineering Task Force, Internet Draft, (Feb. 1998)	
	D639	Exhibit D-3; Aziz et al., U.S. Patent 5,548,646 to Aziz et al., "System for Signatureless Transmission and Reception of Data Packets Between Computer Networks," Filed Sept. 15, 1994 and issued Aug. 20, 1996	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D640	Exhibit D-4; Yinger; U.S. Patent 5,960,204 to Yinger et al., "System and Method for Installing Applications on a Computer on an as needed basis, Filed on October 28, 1996 and Issued September 28, 1999	
	D641	Exhibit D-8; Barlow; U.S. Patent 5,204,961 to Barlow, "Computer Network Operating with Multilevel Hierarchical Security with Selectable Common Trust Realms and Corresponding Security Protocols," Filed on June 25, 1990 and Issued April 20, 1993	
	D642	Exhibit D-12; RFC 1122, Braden, "Requirements for Internet Hosts – Communication Layers," RFC 1122 (Oct. 1989)	
	D643	Exhibit D-13; RFC 791; Information Sciences Institute, "Internet Protocol," DARPA Internet Program Specification RFC 791 (Sept. 1981)	
	D644	Exhibit D-14; Caronni et al., "SKIP – Securing the Internet," 5th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE '96) (June 19-21, 1996)	
	D645	Exhibit D-15; Maughan et al., "Internet Security Association and Key Management Protocol (ISAKMP), " IPSEC Work Group Draft (July 26, 1997)	
	D646	Exhibit E-1; Claim Charts Applying Kiuchi as a Primary Reference to the '759 Patent.	
	D647	Exhibit E-2; Claim Charts Applying Kent as a Primary Reference to the '759 Patent	
	D648	Exhibit E-3; Claim Charts Applying Aziz as a Primary Reference to the '759 Patent	
	D649	Exhibit E-4; Claim Charts Applying Kent in view of Caronni as a Primary Combination of References to the '759 Patent	
	D650	Exhibit D-5; Edwards et al., "High Security Web Servers and Gateways," Computer Networks and ISDN System 29, pages 927-938 (Sept. 1997)	
	D651	Exhibit D-10; Lee et al., "Hypertext Transfer Protocol – HTTP/1.0," RFC 1945 (May 1996)	
	D652	Exhibit E-3; Claim Charts Applying Blum to Claims of the '151 Patent	
	D653	Exhibit B-1, File History of U.S. Patent 7,490,151	
	D654	Exhibit E-1, Claim Charts Applying Kiuchi, and Kiuchi and Martin to Claims of the '151 Patent	
	D655	Exhibit E-2, Claim Charts Applying Wesinger, and Wesinger and Martin to Claims of the '151 Patent	
	D656	Exhibit E-4, Claim Charts Applying Aziz and Edwards, and Aziz, Edwards, and Martin to Claims of the '151 Patent	
	D657	Exhibit E-6, Claim Charts Applying Wesinger and Edwards, and Wesinger, Edwards, and Martin to Claims of the '151 Patent	
	D658	VirnetX Inc., V. Mitel Networks Corp.; Defendants' Joint Invalidity Contentions	
	D659	Exhibit 37, RFC 2661[1] vs. Claims of the '135 Patent [2]	
	D660	Exhibit 38, RFC 2661[1] vs. Claims of the '211 Patent [2]	
	D661	Exhibit 39, RFC 2661[1] vs. Claims of the '504 Patent [2]	
	D662	Exhibit 40, SecureConnect[1] vs. Claims of the '135 Patent [2]	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D663	Exhibit 41, SecureConnect[1] vs. Claims of the '211 Patent [2]	
	D664	Exhibit 42, SecureConnect[1] vs. Claims of the '504 Patent [2]	
	D665	Exhibit 43, SFS-HTTP[1] vs. Claims of the '135 Patent [2]	
	D666	Exhibit 44, SFS-HTTP[1] vs. Claims of the '211 Patent [2]	
	D667	Exhibit 45, SFS-HTTP[1] vs. Claims of the '504 Patent [2]	
	D668	Exhibit 46, US '883[1] vs. Claims of the '135 Patent [2]	
	D669	Exhibit 47, US '883[1] vs. Claims of the '211 Patent [2]	
	D670	Exhibit 48, US '883[1] vs. Claims of the '504 Patent [2]	
	D671	Exhibit 49, Chuah[1] vs. Claims of the '135 Patent [2]	
	D672	Exhibit 50, Chuah[1] vs. Claims of the '211 Patent [2]	
	D673	Exhibit 51, Chuah[1] vs. Claims of the '504 Patent [2]	
	D674	Exhibit 52, U.S. '648[1] vs. Claims of the '135 Patent [2]	
	D675	Exhibit 53, U.S. '648[1] vs. Claims of the '211 Patent [2]	
	D676	Exhibit 57, B&M VPNs[1] vs. Claims of the '504 Patent [2]	
	D677	Exhibit 58, BorderManager[1] vs. Claims of the '135 Patent [2]	
	D678	Exhibit 59, BorderManager[1] vs. Claims of the '211 Patent [2]	
	D679	Exhibit 60, BorderManager[1] vs. Claims of the '504 Patent [2]	
	D680	Exhibit 61, Prestige 128 Plus[1] vs. Claims of the '135 Patent [2]	
	D681	Exhibit 62, Prestige 128 Plus[1] vs. Claims of the '211 Patent [2]	
	D682	Exhibit 63, Prestige 128 Plus[1] vs. Claims of the '504 Patent [2]	
	D683	Exhibit 64, RFC 2401[1] vs. Claims of the '135 Patent [2]	
	D684	Exhibit 65, RFC 2401[1] vs. Claims of the '211 Patent [2]	
	D685	Exhibit 66, RFC 2401[1] vs. Claims of the '504 Patent [2]	
	D686	Exhibit 67, US '072[1] vs. Claims of the '135 Patent [2]	
	D687	Exhibit 68, RFC 2486[1] vs. Claims of the '211 Patent [2]	
	D688	Exhibit 69, RFC 2486[1] vs. Claims of the '504 Patent [2]	

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

	D689	Exhibit 70 Understanding IPSec[1] vs. Claims of the '135 Patent [2]	
	D690	Exhibit 71, Understanding IPSec[1] vs. Claims of the '211 Patent [2]	
	D691	Exhibit 72, Understanding IPSec[1] vs. Claims of the '504 Patent [2]	
	D692	Exhibit 73, US '820[1] vs. Claims of the '135 Patent [2]	
	D693	Exhibit 74, US '820[1] vs. Claims of the '211 Patent [2]	
	D694	Exhibit 75, US '820[1] vs. Claims of the '504 Patent [2]	
	D695	Exhibit 76, US '019[1] vs. Claims of the '211 Patent [2]	
	D696	Exhibit 77, US '019[1] vs. Claims of the '504 Patent [2]	
	D697	Exhibit 78, US '049[1] vs. Claims of the '135 Patent [2]	
	D698	Exhibit 79, US '049[1] vs. Claims of the '211 Patent [2]	
	D699	Exhibit 80, US '049[1] vs. Claims of the '504 Patent [2]	
	D700	Exhibit 81, US '748[1] vs. Claims of the '135 Patent [2]	
	D701	Exhibit 82, US '261[1] vs. Claims of the '135 Patent [2]	
	D702	Exhibit 83, US '261[1] vs. Claims of the '211 Patent [2]	
	D703	Exhibit 84, US '261[1] vs. Claims of the '504 Patent [2]	
	D704	Exhibit 85, US '900[1] vs. Claims of the '135 Patent [2]	
	D705	Exhibit 86, US '900[1] vs. Claims of the '211 Patent [2]	
	D706	Exhibit 87, US '900[1] vs. Claims of the '504 Patent [2]	
	D707	Exhibit 88, US '671[1] vs. Claims of the '135 Patent [2]	
	D708	Exhibit 89, US '671[1] vs. Claims of the '211 Patent [2]	
	D709	Exhibit 90, US '671[1] vs. Claims of the '504 Patent [2]	
	D710	Exhibit 91, JP '704[1] vs. Claims of the '135 Patent [2]	
	D711	Exhibit 92, JP '704[1] vs. Claims of the '211 Patent [2]	
	D712	Exhibit 93, JP '704[1] vs. Claims of the '504 Patent [2]	
	D713	Exhibit 94, GB '841[1] vs. Claims of the '135 Patent [2]	
	D714	Exhibit 95, GB '841[1] vs. Claims of the '211 Patent [2]	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D715	Exhibit 96, GB '841[1] vs. Claims of the '504 Patent [2]	
	D716	Exhibit 97, US '318[1] vs. Claims of the '135 Patent [2]	
	D717	Exhibit 98, US '318[1] vs. Claims of the '211 Patent [2]	
	D718	Exhibit 99, US '318[1] vs. Claims of the '504 Patent [2]	
	D719	Exhibit 100, VPN/VLAN[1] vs. Claims of the '135 Patent [2]	
	D720	Exhibit 101, Nikkei[1] vs. Claims of the '135 Patent [2]	
	D721	Exhibit 102, Nikkei[1] vs. Claims of the '211 Patent [2]	
	D722	Exhibit 103, Nikkei[1] vs. Claims of the '504 Patent [2]	
	D723	Exhibit 104, Special Anthology[1] vs. Claims of the '135 Patent [2]	
	D724	Exhibit 106-A, Gauntlet System[1] vs. Claims of the '135 Patent [2]	
	D725	Exhibit 109-A, Gauntlet System[1] vs. Claims of the '211 Patent [2]	
	D726	Exhibit 110-A, Gauntlet System[1] vs. Claims of the '504 Patent [2]	
	D727	Exhibit 112, IntraPort System[1] vs. Claims of the '135 Patent [2]	
	D728	Exhibit 115, IntraPort System[1] vs. Claims of the '211 Patent [2]	
	D729	Exhibit 116, IntraPort System[1] vs. Claims of the '504 Patent [2]	
	D730	Exhibit 118, Altiga VPN System[1] vs. Claims of the '135 Patent [2]	
	D731	Exhibit 121, Altiga VPN System[1] vs. Claims of the '211 Patent [2]	
	D732	Exhibit 122, Altiga VPN System[1] vs. Claims of the '504 Patent [2]	
	D733	Exhibit 124, Kiuchi[1] vs. Claims of the '135 Patent [2]	
	D734	Exhibit 127, Kiuchi[1] vs. Claims of the '211 Patent [2]	
	D735	Exhibit 128, Kiuchi[1] vs. Claims of the '504 Patent [2]	
	D736	Exhibit 137, Schulzrinne[1] vs. Claims of the '135 Patent [2]	
	D737	Exhibit 137, Schulzrinne[1] vs. Claims of the '135 (Final) Patent [2]	
	D738	Exhibit 140, Schulzrinne[1] vs. Claims of the '211 Patent [2]	
	D739	Exhibit 141, Schulzrinne[1] vs. Claims of the '504 Patent [2]	
	D740	Exhibit 143, Solana[1] vs. Claims of the '135 Patent [2]	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D741	Exhibit 146, Solana[1] vs. Claims of the '211 Patent [2]	
	D742	Exhibit 147, Solana[1] vs. Claims of the '504 Patent [2]	
	D743	Exhibit 155, Marino[1] vs. Claims of the '135 Patent [2]	
	D744	Exhibit 158, Marino[1] vs. Claims of the '211 Patent [2]	
	D745	Exhibit 159, Marino[1] vs. Claims of the '504 Patent [2]	
	D746	Exhibit 168, Aziz[1] vs. Claims of the '135 Patent [2]	
	D747	Exhibit 171, U.S. '234[1] vs. Claims of the '211 Patent [2]	
	D748	Exhibit 172, Aziz[1] vs. Claims of the '504 Patent [2]	
	D749	Exhibit 175, Valencia[1] vs. Claims of the '135 Patent [2]	
	D750	Exhibit 178, Valencia[1] vs. Claims of the '211 Patent [2]	
	D751	Exhibit 179, Valencia[1] vs. Claims of the '504 Patent [2]	
	D752	Exhibit 181, Davison[1] vs. Claims of the '135 Patent [2]	
	D753	Exhibit 184, Davison[1] vs. Claims of the '211 Patent [2]	
	D754	Exhibit 185, Davison[1] vs. Claims of the '504 Patent [2]	
	D755	Exhibit 200, BinGO! User's Guide/Extended Features Reference[1] vs. Claims of the '135 Patent [2]	
	D756	Exhibit 203, Broadband Forum Technical Report TR-025 (Issue 1.0/5.0)[1] vs. Claims of the '135 Patent [2]	
	D757	Exhibit 206, RFC 2230, Key Exchange Delegation Record for the DNS[1] vs. Claims of the '211 Patent [2]	
	D758	Exhibit 207, RFC 2230, Key Exchange Delegation Record for the DNS[1] vs. Claims of the '504 Patent [2]	
	D759	Exhibit 208, RFC 2538, Storing Certificates in the Domain Name System (DNS)[1] vs. Claims of the '211 Patent [2]	
	D760	Exhibit 209, RFC 2538, Storing Certificates in the Domain Name System (DNS)[1] vs. Claims of the '504 Patent [2]	
	D761	Exhibit 212, RFC 2486, RFC 2661, RFC 2401 and Internet-Draft, "Secure Remote Access with L2TP'[1] vs. Claims of the '135 Patent [2]	
	D762	Exhibit 218, U.S. Patent No. 6,496,867 in combination with RFC 2401'[1] vs. Claims of the '135 Patent [2]	
	D763	Exhibit 219, U.S. Patent No. 6,496,867[1] vs. Claims of the '211 Patent [2]	
	D764	Exhibit 220, U.S. Patent No. 6,496,867[1] vs. Claims of the '504 Patent [2]	
	D765	Exhibit 222, U.S. Patent No. 6,557,037[1] vs. Claims of the '211 Patent [2]	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

	D766	Exhibit 223, U.S. Patent No. 6,557,037[1] vs. Claims of the '504 Patent [2]	
	D767	Exhibit 224, RFC 2230, Key Exchange Delegation Record for the DNS[1] vs. Claims of the '135 Patent [2]	
	D768	Exhibit 228, U.S. 588[1] vs. Claims of the '211 Patent [2] (Final)	
	D769	Exhibit 229, U.S. 588[1] vs. Claims of the '504 Patent [2] (Final)	
	D770	Exhibit 230, Microsoft VPN[1] vs. Claims of the '135 Patent [2] (Final)	
	D771	Exhibit 231, Microsoft VPN[1] vs. Claims of the '211 Patent [2] (Final)	
	D772	Exhibit XX, Microsoft VPN[1] vs. Claims of the '504 Patent[2]	
	D773	Exhibit Cisco-1, Cisco's Prior Art System[1] vs. Claims of the '135 Patent[2]	
	D774	Exhibit Cisco-4, Cisco's Prior Art System[1] vs. Claims of the '211 Patent[2]	
	D775	Exhibit Cisco-5, Cisco's Prior Art System[1] vs. Claims of the '504 Patent[2]	
	D776	Exhibit 225, US '037[1] vs. Claims of the '135 Patent[2]	
	D777	Exhibit 226, ITU-T Standardization Activities[1] vs. Claims of the '135 Patent[2]	
	D778	Exhibit 227, US '393[1] vs. Claims of the '135 Patent[2]	
	D779	Exhibit 233, The Miller Application[1] vs. Claim 13 of the '135 Patent[2]	
	D780	Exhibit 234, Aventail Connect 3.1/2.6 Administrator's Guide ("Aventail Connect")[1] vs. Claims of the '504 Patent[2]	
	D781	Exhibit 235, Microsoft VPN[1] vs. Claims of the '504 Patent[2]	
	D782	Exhibit 1, IETF RFC 2065: Domain Name System Security Extensions; published January 1997[1] vs. Claims of the '211 Patent[2]	
	D783	Exhibit 2, IETF RFC 2065: Domain Name System Security Extensions; published January 1997[1] vs. Claims of the '504 Patent[2]	
	D784	Exhibit 3, RFC 2543[1] vs. Claims of the '135 Patent[2]	
	D785	Exhibit 4, RFC 2543[1] vs. Claims of the '211 Patent[2]	
	D786	Exhibit 5, RFC 2543[1] vs. Claims of the '504 Patent[2]	
	D787	Exhibit 6, SIP Draft v.2[1] vs. Claims of the '135 Patent[2]	
	D788	Exhibit 7, SIP Draft v.2[1] vs. Claims of the '211 Patent[2]	
	D789	Exhibit 8, SIP Draft v.2[1] vs. Claims of the '504 Patent[2]	
	D790	Exhibit 9, H.323[1] vs. Claims of the '135 Patent[2]	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D791	Exhibit 10, H.323[1] vs. Claims of the '211 Patent[2]	
	D792	Exhibit 11, H.323[1] vs. Claims of the '504 Patent[2]	
	D793	Exhibit 12, SSL 3.0[1] vs. Claims of the '135 Patent[2]	
	D794	Exhibit 13, SSL 3.0[1] vs. Claims of the '211 Patent[2]	
	D795	Exhibit 14, SSL 3.0[1] vs. Claims of the '504 Patent[2]	
	D796	Exhibit 15, RFC 2487[1] vs. Claims of the '135 Patent[2]	
	D797	Exhibit 16, RFC 2487[1] vs. Claims of the '211 Patent[2]	
	D798	Exhibit 17, RFC 2487[1] vs. Claims of the '504 Patent[2]	
	D799	Exhibit 18, RFC 2595[1] vs. Claims of the '135 Patent[2]	
	D800	Exhibit 21, iPass[1] vs. Claims of the '135 Patent[2]	
	D801	Exhibit 22, iPass[1] vs. Claims of the '211 Patent[2]	
	D802	Exhibit 23, iPass[1] vs. Claims of the '504 Patent[2]	
	D803	Exhibit 24, U.S. Patent No. 6,453,034 ('034 Patent") vs. Claims of the 135 Patent[1]	
	D804	Exhibit 25, U.S. Patent No. 6,453,034 ('034 Patent") vs. Claims of the 211 Patent[1]	
	D805	Exhibit 26, U.S. Patent No. 6,453,034 ('034 Patent") vs. Claims of the 504 Patent[1]	
	D806	Exhibit 27, U.S. Patent No. 6,223,287 ("287 Patent") vs. Claims of the 135 Patent[1]	
	D807	Exhibit 28, U.S. Patent No. 6,223,287 ("287 Patent") vs. Claims of the 211 Patent[1]	
	D808	Exhibit 29, U.S. Patent No. 6,223,287 ("287 Patent") vs. Claims of the 504 Patent[1]	
	D809	Exhibit 35, RFC 1928[1] vs. Claims of the '211 Patent[2]	
	D810	Exhibit 36, RFC 1928[1] vs. Claims of the '504 Patent[2]	
	D811	Exhibit 106, Gaunlet System and Gaunlet References[1] vs. Claims of the '135 Patent[2]	
	D812	Exhibit 109, Gaunlet System and Gaunlet References[1] vs. Claims of the '211 Patent[2]	
	D813	Exhibit 110, Gaunlet System[1] vs. Claims of the '504 Patent[2]	
	D814	Exhibit 130, Overview of Access VPNs and Tunneling Technologies ("Overview")[1] vs. Claims of the '135 Patent[2]	
	D815	Exhibit 133, Overview of Access VPNs and Tunneling Technologies ("Overview")[1] vs. Claims of the '211 Patent[2]	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

	D816	Exhibit 134, Overview of Access VPNs and Tunneling Technologies ("Overview")[1] vs. Claims of the '504 Patent[2]	
	D817	Exhibit 149, Atkinson[1] vs. Claims of the '135 Patent[2]	
	D818	Exhibit 152, Atkinson[1] vs. Claims of the '211 Patent[2]	
	D819	Exhibit 153, Atkinson[1] vs. Claims of the '504 Patent[2]	
	D820	Exhibit 162, Wesinger[1] vs. Claims of the '135 Patent[2]	
	D821	Exhibit 165, Wesinger[1] vs. Claims of the '211 Patent[2]	
	D822	Exhibit 166, Wesinger[1] vs. Claims of the '504 Patent[2]	
	D823	Exhibit 187, AutoSOCKS v2.1[1] vs. Claims of the '135 Patent[2]	
	D824	Exhibit 191, Aventail Connect 3.01/2.51 ("Aventail Connect")[1] vs. Claims of the '135 Patent[2]	
	D825	Exhibit 195, Aventail Connect 3.1/2.6 Administrator's Guide ("Aventail Connect")[1] vs. Claims of the '135 Patent[2]	
	D826	Exhibit 204, Domain Name System (DNS) Security[1] vs. Claims of the '211 Patent[2]	
	D827	Exhibit 205, Domain Name System (DNS) Security[1] ("DNS Security") vs. Claims of the '504 Patent[2]	
	D828	Exhibit 210, Lendenmann[1] vs. Claims of the '211 Patent[2]	
	D829	Exhibit 211, Lendenmann[1] vs. Claims of the '504 Patent[2]	
	D830	Exhibit 213, U.S. Patent No. 7,100,195 in combination with RFC 2401 and U.S. Patent No. 6,496,867[1] vs. Claims of the '135 Patent[2]	
	D831	Exhibit 215, Aziz[1] vs. Claims of the '135 Patent[2]	
	D832	Cisco '180, Efiling Acknowledgment	
	D833	Exhibit A, U.S. Patent 7,188,180	
	D834	Exhibit B1, File History of U.S. Patent 7,188,180	
	D835	Exhibit B2, File History of U.S. Patent Application No. 09/588,209	
	D836	Exhibit B3, File History of Reexamination Control No. 95/001,270, Reexamination of U.S. 7,188,180 requested by Microsoft Corp	
	D837	Exhibit D1, "Lendenmann": Rolf Lendenman, Understanding OSF DCE 1.1 For AIX and OS/2, IBM International Technical Support Organization (Oct. 1995).	
	D838	Exhibit D5, "Schneier": Bruce Schneier, Applied Cryptography (1996)	
	D839	Exhibit D6, RFC 793; Information Sciences Institute, "Transmission Control Protocol," DARPA Internet Program Specification RFC 793 (Sept. 1981)	
	D840	Exhibit D7, "Schimpf"; Brian C. Schimpf, "Securing Web Access with DCE," Presented at Network and Distributed System Security (Feb. 10-11, 1997)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D841	Exhibit D8, "Rosenberry"; Ward Rosenberry, David Kenney, and Gerry Fisher, Understanding DCE (1993)	
	D842	Exhibit D9, Masys; Daniel R. Masys & Dixie B. Baker, "Protecting Clinical Data on Web Client Computers: The PCASSO Approach," Proceedings of the AMIA '98 Annual Symposium, Orlando, Florida (Nov. 7-11, 1998)	
	D843	Exhibit E1, Claim Charts Applying Lendenmann as a Primary Reference to the '180 Patent.	
	D844	Exhibit E2, Claim Charts Applying Kiuchi as a Primary Reference to the '180 Patent	
	D845	Exhibit E3, Claim Charts Applying Solana as a Primary Reference to the '180 Patent	
	D846	Exhibit E4, Claim Charts Applying Schimpf and Rosenberry as a Primary Reference to the '180 Patent	
	D847	Request for Inter Partes Reexamination of Patent No. 7,188,180	
	D848	Modified PTO Form 1449	
	D849	Request for Inter Partes Reexamination Transmittal Form No. 7,188,180	
	D850	Exhibit A; U.S. Patent 7,921,211 with Terminal Disclaimer	
	D851	Exhibit B, Certificate of Service to Request For Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 7,921,211)	
	D852	Exhibit C1, Claim Chart – USP 7,921,211 Relative to Solana, Alone and in Conjunction with RFC 920, Reed and Beser	
	D853	Exhibit C2, Claim Chart – USP 7,921,211 Relative to Solana in view of RFC 2504 and Further in conjunction with RFC 920, Reed, and Beser	
	D854	Exhibit C3, Claim Chart – USP 7,921,211 Relative to Provino, Alone and in Conjunction with RFC 920, Reed, and Beser)	
	D855	Exhibit C4, Claim Chart – USP 7,921,211 Relative to Provino in view of RFC 2230 and Further in Conjunction with RFC 920, Reed and Beser	
	D856	Exhibit C5, Claim Chart – USP 7,921,211 Relative to Provino in view of RFC 2504 and in Further Conjunction with RFC 920, Reed and Beser	
	D857	Exhibit C6, Claim Chart – USP 7,921,211 Relative to Beser, Alone and in Conjunction with RFC 920, RFC 2401, and Reed	
	D858	Exhibit C7, Claim Chart – USP 7,921,211 Relative to RFC 2230, Alone and in Conjunction with RFC 920, RFC 2401, Reed, and Beser	
	D859	Exhibit C8, Claim Chart – USP 7,921,211 Relative to RFC 2538, Alone and in Conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D860	Exhibit D1, Asserted Claim and Infringement Contentions by Plaintiff VirnetX, Inc. in *VirnetX, Inc. v. Cisco Systems, Inc., Apple Inc., Aastra Technologies Ltd, NEC Corporation, NEC Corporation of America and Aastra USA, Inc.*, Civ. Act 6:2010cv00417 (E.D. Tex)	
	D861	Exhibit D2, Asserted Claims and Infringement Contentions by Plaintiff VirnetX, Inc. against Apple based on 7,921,211 Patent	
	D862	Exhibit X1, Solana, E. et al. "Flexible Internet Secure Transactions Based on Collaborative Domains"	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D863	Exhibit X2, U.S. Patent 6,557,037	
	D864	Exhibit X4, Atkinson, R., IETF RFC 2230, "Key Exchange Delegation Record for the DNS" (November 1997)	
	D865	Exhibit X6, Kent, et al., IETF RFC 2401, "Security Architecture for the Internet Protocol" (November 1998) Is Accessible at: http://www.ietf.org/rfc/rfc2401.txt	
	D866	Exhibit X7, Eastlake, D. et al., IETF RFC 2065, "Domain Name System Security Extensions" (January 1997) Is Accessible at: http://www.ietf.org/rfc/rfc2065.txt	
	D867	Exhibit X9, Guttman, E. et al., IETF RFC 2504, "Users' Security Handbook" (February 1999) Is Accessible At: http://www.ietf.org/rfc/rfc2504.txt	
	D868	Exhibit Y3, Braden, R., RFC 1123, "Requirements for Internet Hosts – Application and Support," October 1989 ("RFC1123").	
	D869	Exhibit Y4, Atkinson, R., RFC 1825, "Security Architecture for the Internet Protocol (August 1995) Is Accessible At: http://www.ietf.org/rfc/rfc1825.txt	
	D870	Exhibit Y5, Housley, R. et al., RFC 2459, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" (January 1999) Is accessible At: http://www.ietf.org/rfc/rfc2459.txt	
	D871	Exhibit A, U.S. Patent 7,418,504	
	D872	Exhibit B, Certificate of Service to Request For Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No. 7,418,504)	
	D873	Exhibit C1, Claim Chart – USP 7,418,504 Relative to Solana, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D874	Exhibit C2, Claim Chart – USP 7,418,504 Relative to Solana in view of RFC 2504 and Further in Conjunction with RFC 920, Reed, and Beser	
	D875	Exhibit C3, Claim Chart – USP 7,418,504 Relative to Provino, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D876	Exhibit C4, Claim Chart – USP 7,418,504 Relative to Provino in View of RFC 2230 and Further in Conjunction with RFC 920, Reed and Beser	
	D877	Exhibit C5, Claim Chart – USP 7,418,504 Relative to Provino in View of RFC 2504 and in Further Conjunction with RFC 920, Reed, and Beser	
	D878	Exhibit C6, Claim Chart – USP 7,418,504 Relative to Beser, Alone and in Conjunction with RFC 920, RFC 2401, and Reed	
	D879	Exhibit C7, Claim Chart – USP 7,418,504 Relative to RFC 2230, Alone and in Conjunction with RFC 920, RFC 2401, Reed, and Beser	
	D880	Exhibit C8, Claim Chart – USP 7,418,504 Relative to RFC 2538, Alone and in Conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D881	Exhibit D1, Asserted Claims and Infringement Contentions by Plaintiff VirnetX Inc. in *VimetX, Inc. v. Cisco Systems, Inc., Applce, Inc, Aastra Technologies Ltd., NEC Corporation, NEC Corporation of America and Aastra USA, Inc.*, Civ. Act. 6:2010cv00417 (E.D. Tex)	
	D882	Exhibit D2, Asserted Claims and Infringement Contentions by Plaintiff VirnetX Inc. against Apple Inc. Based on the 7,418,504	
	D883	Exhibit X5, Eastlake, D., et al., IETF RFC 2538, "Storing Certificates in the Domain Name System (DNS)" (March 1999)	
	D884	Exhibit X6, Kent, S. IETF RFC 2401, "Security Architecture for the Internet Protocol, (November1998) http://www.ietf.org/rfc/rfc2401.txt	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D885	Exhibit X8, Postel, J. et al., IETF RFC 920, "Domain Requirements" (October 1984) Is Accessible at http://www.ietf.org/rfc/rfc920.txt	
	D886	Exhibit X10, Reed, M. et al. "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA, Dec. 9-13, 1996.	
	D887	Request for Inter Partes Reexamination Transmittal form	
	D888	Transmittal Letter	
	D889	Request for Inter Partes Reexamination Under 35 U.S.C. § 311	
	D890	Exhibit D-7, "Thomas": Brian Thomas, "Recipe for E-Commerce, IEEE Internet Computing, (Nov.-Dec. 1997)	
	D891	Exhibit D-9, "Kent II": Stephen Kent & Randall Atkinson, "IP Encapsulating Security Payload (ESP)," Internet Engineering Task Force, Internet Draft (Feb. 1998)	
	D892	Exhibit C1, Claim Chart – USP 7,921,211 Relative to Solana, Alone and in Conjunction with RFC 920, Reed and Beser (Came from Inval. Cisco dtd 11/18/11)	
	D893	Exhibit C2, Claim Chart – USP 7,921,211 Relative to Solana in View of RFC 2504 and Further in Conjunction with RFC 920, Reed, and Beser	
	D894	Exhibit C3, Claim Chart – USP 7,921,211 Relative to Provino, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D895	Exhibit C4, Claim Chart – USP 7,921,211 Relative to Provino in View of RFC 2230 and Further in Conjunction with RFC 920, Reed and Beser	
	D896	Exhibit C5, Claim Chart – USP 7,921,211 Relative to Provino in View of RFC 2504 and in Further Conjunction with RFC 920, Reed and Beser	
	D897	Exhibit C6, Claim Chart – USP 7,921,211 Relative to Beser, Alone and in Conjunction with RFC 920, RFC 2401, and Reed	
	D898	Exhibit C7, Claim Chart – USP 7,921,211 Relative to RFC 2230, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D899	Exhibit C8, Claim Chart – USP 7,921,211 Relative to RFC 2538, Alone and in Conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D900	211 Request for Inter Partes Reexamination	
	D901	Exhibit C1, Claim Chart – USP 7,418,504 Relative to Solana, Alone and in Conjunction with RFC 920, Reed and Beser	
	D902	Exhibit C2, Claim Chart – USP 7,418,504 Relative to Solana in View of RFC 2504 and Further in Conjunction with RFC 920, Reed, and Beser	
	D903	Exhibit C3, Claim Chart – USP 7,418,504 Relative to Provino, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D904	Exhibit C5, Claim Chart – USP 7,418,504 Relative to Provino in View of RFC 2504 and in Further Conjunction with RFC 920, Reed and Beser	
	D905	Exhibit C6, USP 7,418,504 Relative to Beser, Alone and in Conjunction with RFC 920, RFC 2401, and Reed	
	D906	Exhibit C7, Claim Chart – USP 7,418,504 Relative to RFC 2230, Alone and in Conjunction with RFC 920, RFC 2401, Reed, and Beser	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

	D907	Exhibit C8, Claim Chart – USP 7,418,504 Relative to RFC 2538, Alone and in Conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D908	504 Request for Inter Partes Reexamination	
	D909	Defendants' Supplemental Joint Invalidity Contentions	
	D910	Exhibit 226, Securing Web Access with DCE[1] vs. Claims of the '135 Patent[2]	
	D911	Exhibit 227, Securing Web Access with DCE[1] vs. Claims of the '151 Patent[2]	
	D912	Exhibit 228, Understanding OSF DCE 1.1 for AIX and OS/2[1] vs. Claims of the '135 Patent[2]	
	D913	Exhibit 229, Understanding OSF DCE 1.1 for AIX and OS/2[1] vs. Claims of the '151 Patent[2]	
	D914	Exhibit 230, Understanding OSF DCE 1.1 for AIX and OS/2[1] vs. Claims of the '180 Patent[2]	
	D915	Exhibit 231, Understanding OSF DCE 1.1 for AIX and OS/2[1] vs. Claims of the '211 Patent[2]	
	D916	Exhibit 232, Understanding OSF DCE 1.1 for AIX and OS/2[1] vs. Claims of the '504 Patent[2]	
	D917	Exhibit 233, Understanding OSF DCE 1.1 for AIX and OS/2[1] vs. Claims of the '759 Patent[2]	
	D918	Exhibit 234, U.S. '648[1] vs. Claims of the '135 Patent	
	D919	Exhibit 235, U.S. '648[1] vs. Claims of the '211 Patent	
	D920	Exhibit 236, U.S. '648[1] vs. Claims of the '504 Patent[2]	
	D921	Exhibit 237, U.S. '648[1] vs. Claims of the '135 Patent[2]	
	D922	Exhibit 238, Gauntlet System [1] vs. Claims of the '211 Patent[2]	
	D923	Exhibit 239, Gauntlet System [1] vs. Claims of the '504 Patent[2]	
	D924	Exhibit 240, Gauntlet System [1] vs. Claims of the '135 Patent[2]	
	D925	Exhibit 241, U.S. '588 [1] vs. Claims of the '211 Patent[2]	
	D926	Exhibit 242, U.S. '588 [1] vs. Claims of the '504 Patent[2]	
	D927	Exhibit 243, Microsoft VPN [1] vs. Claims of the '135 Patent[2]	
	D928	Exhibit 244, Microsoft VPN [1] vs. Claims of the '211 Patent[2]	
	D929	Exhibit 245, Microsoft VPN [1] vs. Claims of the '504 Patent[2]	
	D930	Exhibit 246, ITU-T Standardization Activities [1] vs. Claims of the '135 Patent[2]	
	D931	Exhibit 247, U.S. '393 [1] vs. Claims of the '135 Patent[2]	
	D932	Exhibit 248, The Miller Application [1] vs. Claim 13 of the '135 Patent[2]	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

	D933	Exhibit 249, Gauntlet System [1] vs. Claims of the '151 Patent[2]	
	D934	Exhibit 250, ITU-T Standardization Activities [1] vs. Claims of the '151 Patent[2]	
	D935	Exhibit 251, U.S. Patent No. 5,940,393 [1] vs. Claims of the '151 Patent[2]	
	D936	Exhibit 252, Microsoft VPN [1] vs. Claims of the '151 Patent[2]	
	D937	Exhibit 253, U.S. Patent No.6,324,648 [1] vs. Claims of the '151 Patent[2]	
	D938	Exhibit 254, U.S. Patent No.6,857,072 [1] vs. Claims of the '151 Patent[2]	
	D939	Exhibit A, Aventail Press Release, May 2, 1997	
	D940	Exhibit B, InfoWorld, "Aventail Delivers Highly Secure, Flexible VPN Solution," InfoWorld, page 64D, (1997)	
	D941	Exhibit C, Aventail AutoSOCKS v2.1 Administrator's Guide	
	D942	Exhibit D, Aventail Press Release, October 12, 1998	
	D943	Exhibit G, Aventail Press Release, May 26, 1999	
	D944	Exhibit H, Aventail Press Release, August 9, 1999	
	D945	Exhibit J, "Aventail ExtraNet Center 3.1: Security with Solid Management, Network Computing, June 28, 1999	
	D946	Petition in Opposition to Patent Owner's Petition to Vacate Inter Partes ReExamination Determination on Certain Prior Art	
	D947	Request for Inter Partes Reexamination Under 35 U.S.C. § 311	
	D948	Exhibit B, Certificate of Service to Request for Inter Partes Reexamination Under U.S.C. § 311	
	D949	Exhibit C1, Claim Chart Aventail Connect v3.1	
	D950	Exhibit C2, Claim Chart Aventail Connect v3.01	
	D951	Exhibit C3, Claim Chart Aventail AutoSOCKS	
	D952	Exhibit C4, Claim Chart Wang	
	D953	Exhibit C5, Claim Chart Beser	
	D954	Exhibit C6, Claim Chart BINGO	
	D955	Exhibit X6, U.S. Patent 6,496,867	
	D956	Exhibit X10, U.S. Patent 4,885,778	
	D957	Exhibit X11, U.S. Patent 6,615,357	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D958	Exhibit Y3, U.S. Patent 5,950,519	
	D959	Request for Inter Partes Reexamination Transmittal Form	
	D960	Transmittal Letter	
	D961	Exhibit D, v3.1 Administrator's Guide	
	D962	Exhibit E-1, Claim Charts Applying Kiuchi to Various Claims of the '135 Patent	
	D963	Exhibit E-2, Claim Charts Applying Wesinger to Various Claims of the '135 Patent	
	D964	Exhibit E-3, Claim Charts Applying Solana to Various Claims of the '135 Patent	
	D965	Exhibit E-4, Claim Charts Applying Aziz to Various Claims of the '135 Patent	
	D966	Request for Inter Partes Reexamination Transmittal Form	
	D967	Request for Inter Partes Reexamination	
	D968	Request for Inter Partes Reexamination Transmittal Form 1449/PTO	
	D969	Exhibit C1, Claim Chart Aventail Connect v3.01	
	D970	Exhibit C2, Claim Chart Aventail AutoSOCKS	
	D971	Exhibit C3, Claim Chart BINGO	
	D972	Exhibit C4, Claim Chart Beser	
	D973	Exhibit C5, Claim Chart Wang	
	D974	Transmittal Letter	
	D975	Request for Inter Partes Reexamination Under 35 U.S.C. § 311	
	D976	Exhibit B, Certificate of Service to Request for Inter Partes Reexamination Under 35 U.S.C. § 311	
	D977	Exhibit E-1, Claim Charts Applying Kiuchi, and Kiuchi and Martin to Claims of the '151 Patent	
	D978	Exhibit E-2, Claim Charts Applying Wesinger, and Wesinger and Martin to Claims of the '151 Patent	
	D979	Exhibit E-3, Claim Charts Applying Blum to Claims of the '151 Patent	
	D980	Exhibit E-4, Claim Charts Applying Aziz and Edwards, and Aziz, Edwards, and Martin to Claims of the '151 Patent	
	D981	Exhibit E-5, Claim Charts Applying Kiuchi and Edwards, and Kiuchi, Edwards, and Martin to Claims of the '151 Patent	
	D982	Exhibit E-6, Claim Charts Applying Wesinger and Edwards, and Wesinger, Edwards, and Martin to Claims of the '151 Patent	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D983	Exhibit A, U.S. Patent 6,839,759	
	D984	Exhibit C-1, U.S. Patent 6,502,135	
	D985	Exhibit E-1, Claim Charts Applying Kiuchi, as Primary Reference to the '759 Patent	
	D986	Exhibit E-2, Claim Charts Applying Kent as a Primary Reference to the '759 Patent	
	D987	Exhibit E-3, Claim Charts Applying Aziz as a Primary Reference to the '759 Patent	
	D988	Exhibit E-4, Claim Charts Applying Kent in View of Caronni as a Primary Combination of References to the '759 Patent	
	D989	Request for Inter Partes Reexamination Transmittal Form	
	D990	Request for Inter Partes Reexamination	
	D991	Request for Inter Partes Reexamination Transmittal(form 1449/PTO)	
	D992	Certificate of Service to Request for Inter Partes Reexamination Under 35 U.S.C. § 311	
	D993	Request for Inter Partes Reexamination	
	D994	Request for Inter Partes Reexamination Transmittal Form	
	D995	Request for Inter Partes Reexamination	
	D996	Request for Inter Partes Reexamination Transmittal Form	
	D997	Exhibit C1, Claim Chart – USP 7,921,211 Relative to Solana, Alone and in Conjunction with RFC 920, Reed and Beser	
	D998	Exhibit C2, Claim Chart – USP 7,921,211 Relative to Solana in view of RFC 2504 and Further in conjunction with RFC 920, Reed, and Beser	
	D999	Exhibit C3, Claim Chart – USP 7,921,211 Relative to Provino, Alone and in Conjunction with RFC 920, Reed, and Beser	
	D1000	Exhibit C4, Claim Chart – USP 7,921,211 Relative to Provino in view of RFC 2230 and Further in Conjunction with RFC 920, Reed and Beser	
	D1001	Exhibit C5, Claim Chart – USP 7,921,211 Relative to Provino in view of RFC 2504 and in Further Conjunction with RFC 920, Reed and Beser	
	D1002	Exhibit C6, Claim Chart – USP 7,921,211 Relative to Beser, Alone and in Conjunction with RFC 920, RFC 2401, and Reed	
	D1003	Exhibit C7, Claim Chart – USP 7,921,211 Relative to RFC 2230, Alone and in Conjunction with RFC 920, RFC 2401, Reed, and Beser	
	D1004	Exhibit C8, Claim Chart – USP 7,921,211 Relative to RFC 2538, Alone and in Conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D1005	Exhibit D1, Asserted Claim and Infringement Contentions by Plaintiff VirnetX, Inc. in *VirnetX, Inc. v. Cisco Systems, Inc., Apple Inc., Aastra Technologies Ltd, NEC Corporation, NEC Corporation of America and Aastra USA, Inc.*, Civ. Act 6:2010cv00417 (E.D. Tex)	
	D1006	Exhibit D2, Asserted Claims and Infringement Contentions by Plaintiff VirnetX, Inc. against Apple based on 7,921,211 Patent	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D1007	Exhibit B1, File History of U.S. Patent 7,418,504	
	D1008	Exhibit B2, File History of U.S. Patent Application No. 09/558,210	
	D1009	Exhibit D-10, Gaspoz et al., "VPN on DCE: From Reference Configuration to Implementation," Bringing Telecommunication Services to the People – IS&N '95, Third International Conference on Intelligence in Broadband Services and Networks, October 1995 Proceedings, Lecture Notes in Computer Science, Vol. 998 (Springer, 1995)	
	D1010	Exhibit D-11, Copy of U.S. Patent No. 6,269,099	
	D1011	Exhibit D-11, Copy of U.S. Patent No. 6,560,634	
	D1012	Exhibit D-13, Pallen, "The World Wide Web," British Medical Journal, Vol. 311 at 1554 (Dec. 1995)	
	D1013	Exhibit D-14, Rivest et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, 21:120-126 (Feb. 1978)	
	D1014	Exhibit D-15, Copy of U.S. Patent No. 4,952,930	
	D1015	Exhibit D-17, Pfaffenberger, Netscape Navigator 3.0: Surfing the Web and Exploring the Internet, Academic Press (1996)	
	D1016	Exhibit D-18, Gittler et al., "The DCE Security Service," Hewlett-Packard Journal, pages 41-48 (Dec. 1995)	
	D1017	Exhibit D-6, Copy of U.S. Patent No. 5,689,641	
	D1018	Exhibit D-9, Lawton, "New Top-Level Domains Promise Descriptive Names," Sunworld Online, 1996	
	D1019	Exhibit E-1, Copy of Catalog Listing by IBM for RS/6000 Redbooks Collection which includes a Link to the *Lendenmann* reference. The link to the *Lendenmann* reference was archived at archive.org on December 7, 1998 and retrieved by the Wayback Machine	
	D1020	Exhibit E-10, copy of an Archived Version of the Lawton reference archived at archive.org on February 19, 1999 and retrieved by the Wayback Machine	
	D1021	Exhibit E-11, Abstracts of the Proceedings of the Symposium on Network and Distributed System Security, 1996, Archived at archive.org on April 10, 1997, and retrieved by the Wayback Machine	
	D1022	Exhibit E-12, 1996 Symposium on Network and Distributed System Security, Website Archived by archive.org (Apr. 10, 1997), Retrieved by the Wayback Machine at http://web.archive.org/web/19970410114853/http://computer.org/cspress/catalog/proc9.htm.	
	D1023	Exhibit E-13, Copy of Search Results for ISBN 0-12-553153-2 (Pfaffenberger) from www.isbnsearch.org	
	D1024	Exhibit F-1, Claim Charts applying Lendenmann as a Primary Reference to the '504 Patent.	
	D1025	Exhibit F-2, Claim Charts applying Aziz as a Primary Reference to the '504 Patent	
	D1026	Exhibit F-3, Claim Charts applying Kiuchi and Pfaffenberger as Primary References to the '504 Patent	
	D1027	Exhibit E-2, First Page of U.S. Patent No. 5,913,217 published June 15, 1999 and citing a portion of the Lendenmann reference as a prior art reference	
	D1028	Exhibit E-3, Request for Comments 2026, "The Internet Standards Process – Revision 3," October 1996	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D1029	Exhibit E-4, First Page of U.S. 5,463,735, published October 31, 1995 and citing RFC 793 as a prior art Reference	
	D1030	Exhibit E-5, Copy of catalog listing from Boston University Digital Common Website, listing the Martin reference with an issue date of February 21, 1998	
	D1031	Exhibit E-6, Copy of Technical Reports Archive Listing from Boston University Computer Science Department which includes a link to the Martin paper. The link to the Martin paper was archived at archive.org on January 22, 1998 and Retrieved by the Wayback Machine	
	D1032	Exhibit E-7, Boston University Computer Science Department Technical Reports Instructions, available at: http://www.cs.bu.edu/techreports/INSTRUCTIONS	
	D1033	Exhibit E-8, U. Möller, "Implementation eines Anonymisierungsverfahrens für WWW-Zugriffe," Diplomarbeit, Universität Hamburg (July 16, 1999), citing to Martin at page 77.	
	D1034	Exhibit E-9, First page of U.S. 5,737,423, published April 7, 1998 and citing Schneier as Prior Art Reference	
	D1035	Request for Inter Partes ReExamination; U.S. Patent 7,418,504	
	D1036	Request for Inter Partes ReExamination Transmittal Form; U.S. Patent 7,418,504	
	D1037	Request for Inter Partes Reexamination Transmittal (Form 1449/PTO) 7,418,504	
	D1038	Exhibit C1, Claim Chart – USP 7,921,211 relative to Solana, alone and in conjunction with RFC 920, Reed and Beser	
	D1039	Exhibit C2, Claim Chart – USP 7,921,211 relative to Solana in view of RFC 2504 and further in conjunction with RFC 920, Reed, and Beser	
	D1040	Exhibit C3, Claim Chart – USP 7,921,211 relative to Provino, alone and in conjunction with RFC 920, Reed, and Beser	
	D1041	Exhibit C4, Claim Chart – USP 7,921,211 relative to Provino in view of RFC 2230 and further in conjunction with RFC 920, Reed and Beser	
	D1042	Exhibit C5, Claim Chart – USP 7,921,211 relative to Provino in view of RFC 2504 and in further conjunction with RFC 920, Reed and Beser	
	D1043	Exhibit C6, Claim Chart – USP 7,921,211relative to Beser, Alone and in conjunction with RFC 920, RFC 2401, and Reed	
	D1044	Exhibit C7, Claim Chart – USP 7,921,211 relative to RFC 2230, alone and in conjunction with RFC 2401, Reed, and Beser	
	D1045	Exhibit C8, Claim Chart – USP 7,921,211 relative to RFC 2538, alone and in conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D1046	Request for Inter Partes Reexamination under 35 U.S.C. § 311	
	D1047	Exhibit C1, Claim Chart – USP 7,418,504 relative to Solana, alone and in conjunction with RFC 920, Reed and Beser	
	D1048	Exhibit C2, Claim Chart – USP 7,418,504 relative to Solana in view of RFC 2504 and further in conjunction with RFC 920, Reed, and Beser	
	D1049	Exhibit C3, Claim Chart – USP 7,418,504 relative to Provino, alone and in conjunction with RFC 920, Reed, and Beser	
	D1050	Exhibit C5, Claim Chart – USP 7,418,504 relative to Provino in view of RFC 2504 and in further conjunction with RFC 920, Reed and Beser	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D1051	Exhibit C6, USP 7,418,504 relative to Beser, alone and in conjunction with RFC 920, RFC 2401, and Reed	
	D1052	Exhibit C7, Claim Chart – USP 7,418,504 relative to RFC 2230, alone and in conjunction with RFC 920, RFC 2401, Reed, and Beser	
	D1053	Exhibit C8, Claim Chart – USP 7,418,504 relative to RFC 2538, alone and in conjunction with RFC 920, RFC 2401, Reed, Beser, and RFC 2065	
	D1054	Request for Inter Partes Reexamination under 35 U.S.C. § 311	
	D1055	Exhibit 226, Securing Web Access with DCE[1] vs. Claims of the '135 Patent[2]	
	D1056	Exhibit 227, Securing Web Access with DCE[1] vs. Claims of the '151 Patent[2]	
	D1057	Exhibit 228, Understanding OSF DCE 1.1 for AIX and OS/2[1] vs. Claims of the '135 Patent[2]	
	D1058	Exhibit 229, Understanding OSF DCE 1.1 for AIX and OS/2[1] vs. Claims of the '151 Patent[2]	
	D1059	Exhibit 230, Understanding OSF DCE 1.1 for AIX and OS/2[1] vs. Claims of the '180 Patent[2]	
	D1060	Exhibit 231, Understanding OSF DCE 1.1 for AIX and OS/2[1] vs. Claims of the '211 Patent[2]	
	D1061	Exhibit 232, Understanding OSF DCE 1.1 for AIX and OS/2[1] vs. Claims of the '504 Patent[2]	
	D1062	Exhibit 233, Understanding OSF DCE 1.1 for AIX and OS/2[1] vs. Claims of the '759 Patent[2]	
	D1063	Exhibit 234, U.S. '648[1] vs. Claims of the '135 Patent[2]	
	D1064	Exhibit 235, U.S. '648[1] vs. Claims of the '211 Patent[2]	
	D1065	Exhibit 236, U.S. '648[1] vs. Claims of the '504 Patent[2]	
	D1066	Exhibit 237, U.S. '072[1] vs. Claims of the '135 Patent[2]	
	D1067	Exhibit 238, Gauntlet System [1] vs. Claims of the '211 Patent[2]	
	D1068	Exhibit 239, Gauntlet System[1] vs. Claims of the '504 Patent[2]	
	D1069	Exhibit 240, Gauntlet System [1] vs. Claims of the '135 Patent[2]	
	D1070	Exhibit 241, U.S. '588 [1] vs. Claims of the '211 Patent[2]	
	D1071	Exhibit 242, U.S. '588 [1] vs. Claims of the '504 Patent[2]	
	D1072	Exhibit 243, Microsoft VPN [1] vs. Claims of the '135 Patent[2]	
	D1073	Exhibit 244, Microsoft VPN [1] vs. Claims of the '211 Patent[2]	
	D1074	Exhibit 245, Microsoft VPN [1] vs. Claims of the '504 Patent[2]	
	D1075	Exhibit 246, ITU-T Standardization Activities[1] vs. Claims of the '135 Patent[2]	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D1076	Exhibit 247, U.S. '393[1] vs. Claims of the '135 Patent[2]	
	D1077	Exhibit 248, The Miller Application[1] vs. Claim 13 of the '135 Patent[2]	
	D1078	Exhibit 249, Gauntlet System [1] vs. Claims of the '151 Patent[2]	
	D1079	Exhibit 250, ITU-T Standardization Activities [1] vs. Claims of the '151 Patent[2]	
	D1080	Exhibit 251, U.S. Patent No. 5,940,393 [1] vs. Claims of the '151 Patent[2]	
	D1081	Exhibit 252, Microsoft VPN [1] vs. Claims of the '151 Patent[2]	
	D1082	Exhibit 253, U.S. Patent No.6,324,648 [1] vs. Claims of the '151 Patent[2]	
	D1083	Exhibit 254, U.S. Patent No.6,857,072 [1] vs. Claims of the '151 Patent[2]	
	D1084	Petition in Opposition to Patent Owner's Petition to Vacate *Inter Partes* Reexamination	
	D1085	Petition in Opposition to Patent Owner's Petition to Vacate *Inter Partes* Reexamination	
	D1086	Petition in Opposition to Patent Owner's Petition to Vacate *Inter Partes* Reexamination	
	D1087	Exhibit B1, File History of U.S. Patent 7,921,211	
	D1088	Exhibit B2, File History of U.S. Patent Application No. 10/714,849	
	D1089	Exhibit B4, *VirnetX, Inc. v. Microsoft Corp.*, Case No. 6:07-cv-80, Memorandum Opinion on Claim Construction (E.D. Tex. Jul. 30, 2009)	
	D1090	Exhibit D15, U.S. Patent 4,952,930	
	D1091	Exhibit F1, Claim Charts Applying Lendenmann as a Primary Reference to the '211 Patent	
	D1092	Exhibit F2, Claim Charts Applying Aziz as a Primary Reference to the '211 Patent	
	D1093	Exhibit F3, Claim Charts Applying Kiuchi and Pfaffenberger as Primary References to the '211 Patent	
	D1094	Exhibit 2, Letter and attachment from Ramzi Khazen, Counsel for VirnetX, to Dmitriy Kheyfits, Counsel for Cisco Systems (June 23, 2011)	
	D1095	Exhibit P, Malkin, "Dial-In Virtual Private Networks Using Layer 3 Tunneling"	
	D1096	Exhibit Q, Ortiz, "Virtual Private Networks: Leveraging the Internet"	
	D1097	Exhibit R, Keromytix, "Creating Efficient Fail-Stop Cryptographic Protocols"	
	D1098	Transcript of Markman Hearing Dated January 5, 2012	
	D1099	Declaration of John P. J. Kelly, Ph.D	
	D1100	Defendants' Responsive Claim Construction Brief; Exhibits A–P and 1-7	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D1101	Joint Claim Construction and Prehearing Statement Dated 11/08/11	
	D1102	Exhibit A: Agreed Upon Terms Dated 11/08/11	
	D1103	Exhibit B: Disputed Claim Terms Dated 11/08/11	
	D1104	Exhibit C: VirnetX's Proposed Construction of Claim Terms and Supporting Evidence Dated 11/08/11	
	D1105	Exhibit D: Defendant's Intrinsic and Extrinsic Support Dated 11/08/11	
	D1106	Declaration of Austin Curry in Support of VirnetX Inc.'s Opening Claim Construction Brief	
	D1107	Declaration of Mark T. Jones Opening Claims Construction Brief	
	D1108	VirnetX Opening Claim Construction Brief	
	D1109	VirnetX Reply Claim Construction Brief	
	D1110	European Search Report from corresponding EP Application Number 11005789 (Our Ref.: 077580-0142)	
	D1111	European Search Report from corresponding EP Application Number 11005792 (Our Ref.: 077580-0143)	

C8

(12) UK Patent Application (19) GB (11) 2 340 702 (13) A

(43) Date of A Publication 23.02.2000

(21) Application No 9912200.4

(22) Date of Filing 25.05.1999

(30) Priority Data
(31) 09087823 (32) 29.05.1998 (33) US

(51) INT CL[7]
H04L 29/06 // H04L 9/00 12/22 12/46

(52) UK CL (Edition R)
H4P PPEB

(56) Documents Cited
EP 0887979 A2 EP 0825748 A2 WO 98/31124 A1

(58) Field of Search
UK CL (Edition Q) H4P PPA PPEB PPEC PPG
INT CL[6] H04L 12/22 12/46 12/66 29/06
ONLINE DATABASES: WPI, EPODOC, JAPIO

(71) Applicant(s)
Sun Microsystems Inc
(Incorporated in USA - Delaware)
901 San Antonio Road, MS Palo Alto-521,
California 94303, United States of America

(72) Inventor(s)
Joseph E Provino

(74) Agent and/or Address for Service
D Young & Co
21 New Fetter Lane, LONDON, EC4A 1DA,
United Kingdom

(54) Abstract Title
Accessing a server in a virtual private network protected by a firewall

(57) A virtual private network 15 has a firewall 30, at least one server 31 and a nameserver 32 each having a network address (eg. an n-bit integer address). The server 31 also has a secondary address (eg. a human readable address) and the nameserver 32 provides an association between the secondary address and the network address. An authorised external device 12 establishes a secure tunnel between itself and the firewall for communication using encryption. When the external device requests connection to server 31 using the secondary address of server 31, the firewall provides external device 12 with the network address of the nameserver 32. The external device 12 transmits a request for resolution of the network address associated with the secondary address to the nameserver through the firewall. The nameserver then transmits the network address of the server 31 through the firewall to the external device using the secure tunnel. The external device can thereafter use the network address of server 31 in subsequent communications.

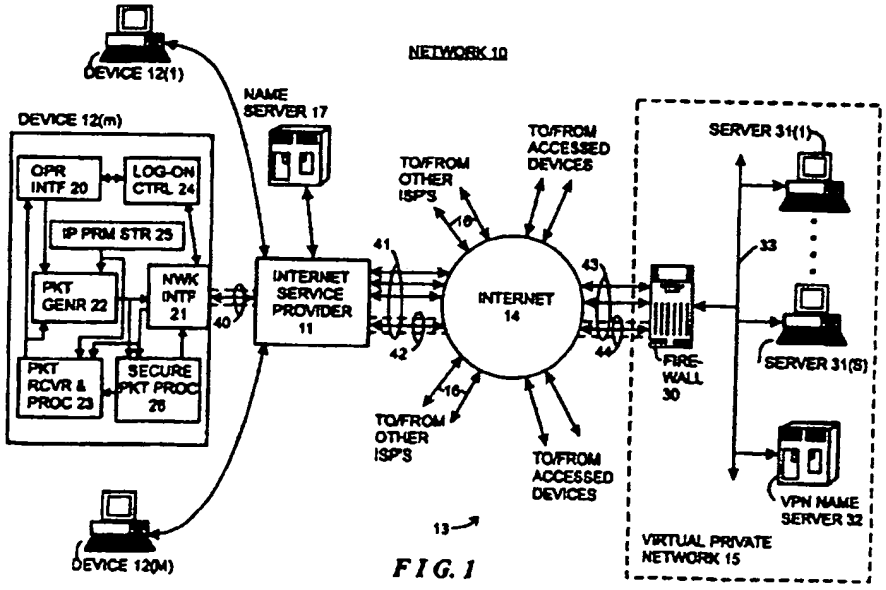


FIG. 1

GB 2 340 702 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

This print takes account of replacement documents submitted after the date of filing to enable the application to comply with the formal requirements of the Patents Rules 1995

Petitioner Apple Inc. - Exhibit 1002, p. 866

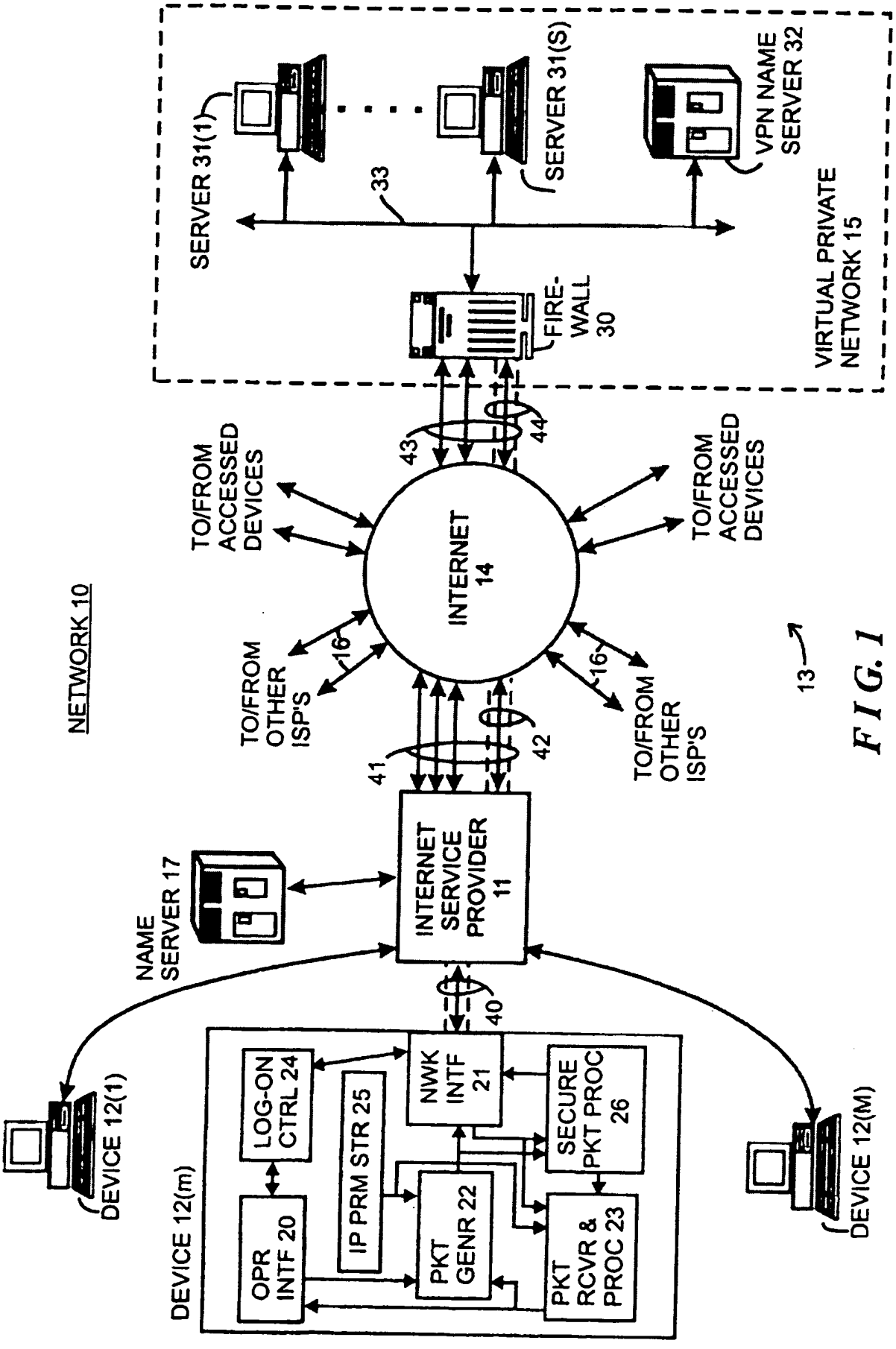

NETWORK 10
VIRTUAL PRIVATE NETWORK 15
SERVER 31(1)
SERVER 31(S)
VPN NAME SERVER 32
33
FIRE-WALL 30
43
44
TO/FROM ACCESSED DEVICES
TO/FROM ACCESSED DEVICES
INTERNET 14
TO/FROM OTHER ISP'S
16
16
TO/FROM OTHER ISP'S
41
42
13
INTERNET SERVICE PROVIDER 11
NAME SERVER 17
40
DEVICE 12(1)
DEVICE 12(m)
DEVICE 12(M)
LOG-ON CTRL 24
NWK INTF 21
SECURE PKT PROC 26
IP PRM STR 25
OPR INTF 20
PKT GENR 22
PKT RCVR & PROC 23

FIG. 1

FIELD OF THE INVENTION

The invention relates generally to the field of digital communications systems and methods, and more particularly to systems and methods for easing communications between devices connected to public networks such as the Internet and devices connected to private networks.

BACKGROUND OF THE INVENTION

Digital networks have been developed to facilitate the transfer of information, including data and programs, among digital computer systems and other digital devices. A variety of types of networks have been developed and implemented, including so-called "wide-area networks" (WAN's) and "local area networks" (LAN's), which transfer information using diverse information transfer methodologies. Generally, LAN's are implemented over relatively small geographical areas, such as within an individual office facility or the like, for transferring information within a particular office, company or similar type of organization. On the other hand, WAN's are generally implemented over relatively large geographical areas, and may be used to transfer information between LAN's as well as between devices that are not connected to LAN's. WAN's also include public networks, such as the Internet, which can carry information for a number of companies.

Several problems have arisen in connection with communication over a network, particularly a large public WAN such as the Internet. Generally, information is transferred over a network in message packets, which are transferred from one device, as a source device, to another device as a destination device, through one or more routers or switching nodes (generally, switching nodes) in the network. Each message packet includes a destination address which the switching nodes use to route the respective message packet to the appropriate destination device. Addresses over the Internet are in the form of an "n"-bit integer (where "n" may be thirty two or 128), which are difficult for a person to remember and enter when he or she wishes to enable a message packet to be transmitted. To relieve a user of the necessity of remembering and entering specific integer Internet

addresses, the Internet provides second addressing mechanism which is more easily utilized by human operators of the respective devices. In that addressing mechanism, Internet domains, such as LAN's, Internet service providers ("ISP's") and the like which are connected in the Internet, are identified by relatively human-readable names. To accommodate the use of human-readable names, nameservers, also referred to as DNS servers, are provided to resolve the human-readable names to the appropriate Internet addresses. When an operator at one device, wishing to transmit a message packet to another device, enters the other device's human-readable name, the device will initially contact a nameserver. Generally, the nameserver may be part of the ISP itself or it may be a particular device which is accessible through the ISP over the Internet; in any case, the ISP will identify the nameserver to be used to the device when the device logs in to the ISP. If, after being contacted by the device, the nameserver has or can obtain an integer Internet address for the human-readable domain name, it (that is, the nameserver) will provide the integer Internet address corresponding to the human-readable domain name to the operator's device. The device, in turn, can thereafter include the integer Internet address returned by the nameserver in the message packet and provide the message packet to the ISP for transmission over the Internet in a conventional manner. The Internet switching nodes use the integer Internet address to route the message packet to the intended destination device.

Other problems arise, in particular, in connection with the transfer of information over a public WAN such as the Internet. One problem is to ensure that information transferred over the WAN that the source device and the destination device wish to maintain confidential, in fact, remains confidential as against possible eavesdroppers which may intercept the information. To maintain confidentiality, various forms of encryption have been developed and are used to encrypt the information prior to transfer by the source device, and to decrypt the information after it has been received by the destination device. If it is desired that, for example, all information transferred between a particular source device and a particular destination device is maintained confidential, the devices can establish a "secure tunnel" therebetween, which essentially ensures that all information to be transferred by the source device to the destination device is encrypted (except for certain

protocol information, such as address information, which controls the flow of network packets through the network between the source and destination devices) prior to transfer, and that the encrypted information will be decrypted prior to utilization by the destination device. The source and destination devices may themselves perform the encryption and decryption, respectively, or the encryption and decryption may be performed by other devices prior to the message packets being transferred over the Internet.

A further problem that arises in particular in connection with companies, government agencies, and private organizations whose private networks, which may be LAN's, WAN's or any combination thereof, are connected to public WAN's such as the Internet, is to ensure that their private networks are secure against others whom the companies do not wish to have access thereto, or to regulate and control access by others whom the respective organizations may wish to have limited access. To accommodate that, the organizations typically connect their private networks to the public WAN's through a limited number of gateways sometimes referred to as "firewalls," through which all network traffic between the internal and public networks pass. Typically, network addresses of domains and devices in the private network "behind" the firewall are known to nameservers which are provided in the private network, but are not available to nameservers or other devices outside of the private network, making communication between a device outside of the private network and a device inside of the private network difficult.

SUMMARY OF THE INVENTION

Particular and preferred aspects of the invention are set out in the accompanying independent and dependent claims. Features of the dependent claims may be combined with those of the independent claims as appropriate and in combinations other than those explicitly set out in the claims.

The invention provides a new and improved system and method for easing communications between devices connected to public networks such as the Internet and devices connected to private networks by facilitating resolution of secondary addresses, such as the Internet's human-readable addresses, to network addresses by nameservers or the like connected to the private networks.

In brief summary, an embodiment of the invention provides a system comprising a virtual private network and an external device interconnected by a digital network. The virtual private network has a firewall, at least one internal device and a nameserver each having a network address. The internal device also has a secondary address, and the nameserver is configured to provide an association between the secondary address and the network address. The firewall, in response to a request from the external device to establish a connection therebetween, provides the external device with the network address of the nameserver. The external device, in response to a request from an operator or the like, including the internal device's secondary address, requesting access to the internal device, generates a network address request message for transmission over the connection to the firewall requesting resolution of the network address associated with the secondary address. The firewall provides the address resolution request to the nameserver, and the nameserver provides the network address associated with the secondary address to the firewall. The firewall, in turn, provides the network address in a network address response message for transmission over the connection to the external device. The external device can thereafter use the network address so provided in subsequent communications with the firewall intended for the internal device.

BRIEF DESCRIPTION OF THE DRAWINGS

Exemplary embodiments of the invention are described hereinafter, by way of example only, with reference to the accompanying drawings, in which:

FIG. 1 is a functional block diagram of a network constructed in accordance with the invention.

DETAILED DESCRIPTION OF AN ILLUSTRATIVE EMBODIMENT

FIG. 1 is a functional block diagram of a network 10 constructed in accordance with the invention. The network 10 as depicted in FIG. 1 includes an Internet service provider ("ISP") 11 which facilitates the transfer of message packets among one or more devices 12(1) through 12(M) (generally identified by reference numeral 12(m)) connected to ISP 11, and other devices, generally identified by reference numeral 13, over the Internet 14, thereby to facilitate the transfer of information in message packets among the devices 12(m) and 13. The ISP 11 connects to the Internet 14 over one or more logical connections or gateways or the like (generally referred to herein as "connections") generally identified by reference numeral 41. The ISP 11 may be a public ISP, in which case it connects to devices 12(m) which may be controlled by operators who are members of the general public to provide access by those operators to the Internet. Alternatively, ISP 11 may be a private ISP, in which case the devices 12(m) connected thereto are generally operated by, for example, employees of a particular company or governmental agency, members of a private organization or the like, to provide access by those employees or members to the Internet.

As is conventional, the Internet comprises a mesh of switching nodes (not separately shown) which interconnect ISP's 11 and devices 13 to facilitate the transfer of message packets thereamong. The message packets transferred over the Internet 14 conform to that defined by the so-called Internet protocol "IP" and include a header portion, a data portion, and may include a error detection and/or correction portion. The header portion includes information used to transfer the message packet through the Internet 14, including, for example, a destination address that identifies the device that is to receive the message packet as the destination device and a source address that identifies the device which generated the message packet. For each message packet, the destination and source addresses are each in the form of an integer that uniquely identifies the respective destination and source devices. The switching nodes comprising the Internet 14 use at least the destination address of each respective message packet to route it (that is, the respective message packet) to the destination device, if the destination device is connected to the Internet, or to an ISP 11 or other device connected to the Internet 14, which, in turn, will forward the message packet to the appropriate destination. The data portion of each message packet includes the data to be transferred

in the message packet, and the error detection and/or correction portion contains error detection and/or correction information which may be used to verify that the message packet was correctly transferred from the source to the destination device (in the case of error detection information), and correct selected types of errors if the message packet was not correctly transferred (in the case of error correction information).

The devices 12(m) connected to ISP 11 may comprise any of a number of types of devices which communicate over the Internet 14, including, for example, personal computers, computer workstations, and the like, with other devices 13. Each device 12(m) communicates with the ISP 11 to transfer message packets thereto for transfer over the Internet 14, or to receive message packets therefrom received by the ISP 11 over the Internet 14, using any convenient protocol such as the well-known point-to-point protocol ("PPP") if the device 12(m) is connected to the ISP 11 using a point-to-point link, any conventional multi-drop network protocol if the device 12(m) is connected to the ISP 11 over a multi-drop network such as the Ethernet, or the like. The devices 12(m) are generally constructed according to the conventional stored-program computer architecture, including, for example, a system unit, a video display unit and operator input devices such as a keyboard and mouse. A system unit generally includes processing, memory, mass storage devices such as disk and/or tape storage elements and other elements (not separately shown), including network and/or telephony interface devices for interfacing the respective device to the ISP 11. The processing devices process programs, including application programs, under control of an operating system, to generate processed data. The video display unit permits the device to display processed data and processing status to the user, and the operator input device enables the user to input data and control processing.

These elements of device 12(m), along with suitable programming, cooperate to provide device 12(m) with a number of functional elements including, for example, an operator interface 20, a network interface 21, a message packet generator 22, a message packet receiver and processor 23, an ISP log-on control 24, an Internet parameter store 25 and, in connection with the invention, a secure message packet processor 26. The operator interface 20 facilitates reception by the device

12(m) of input information from the operator input device(s) of device 12(m) and the display of output information to the operator on the video display device(s) of the device 12(m). The network interface 21 facilitates connection of the device 12(m) to the ISP 11 using the appropriate PPP or network protocol, to transmit message packets to the ISP 11 and receive message packets therefrom. The network interface 21 may facilitate connection to the ISP 11 over the public telephone network to allow for dial-up networking of the device 12(m) over the public telephone system. Alternatively or in addition, the network interface 21 may facilitate connection through the ISP 11 over, for example, a conventional LAN such as the Ethernet. The ISP log on control 24, in response to input provided by the operator interface 20 and/or in response to requests from programs (not shown) being processed by the device 12(m), communicates through the network interface 21 to facilitate the initialization ("log-on") of a communications session between the device 12(m) and the ISP 11, during which communications session the device 12(m) will be able to transfer information, in the form of, message packets with other devices over the Internet 14, as well as other devices 12(m') (m'≠m) connected to the ISP 11 or to other ISP's. During a log-on operation, the ISP log-on control 24 receives the Internet protocol ("IP") parameters which will be used in connection with message packet generation during the communications session.

During a communications session, the message packet generator 22, in response to input provided by the operator through the operator interface 20, and/or in response to requests from programs (not separately shown) being processed by the device 12(m), generates message packets for transmission through the network interface 21. The network interface 21 also receives message packets from the ISP 11 and provides them to message packet receiver and processor 23 for processing and provision to the operator interface 20 and/or other programs (not shown) being processed by the device 12(m). If the received message packets contain information, such as Web pages or the like, which is to be displayed to the operator, the information can be provided to the operator interface 20 to enable the information to be displayed on the device's video display unit. In addition or alternatively, the information may be provided to other programs (not shown) being processed by the device 12(m) for processing.

Generally, elements such as the operator interface 20, message packet generator 22, message packet receiver and processor 23, ISP log-on control 24 and Internet parameter store 25 may comprise elements of a conventional Internet browser, such as Mosaic, Netscape Navigator and Microsoft Internet Explorer.

In connection with the invention, as noted above the device 12(m) also includes a secure message packet processor 26. The secure message packet processor 26 facilitates the establishment and use of a "secure tunnel," which will be described below, between the device 12(m) and another device 12 (m') (m'≠m) or 13. Generally, in a secure tunnel, information in at least the data portion of message packets transferred between device 12(m) and a specific other device 12(m') (m'≠m) or 13 is maintained in secret by, for example, encrypting the data portion prior to transmission by the source device. Information in other portions of such message packets may also be maintained in secret, except for the information that is required to facilitate the transfer of the respective message packet between the devices, including, for example, at least the destination information, so as to allow the Internet's switching nodes and ISP's to identify the device that is to receive the message packet.

In addition to ISP 11, a number of other ISP's may connect to the Internet, as represented by arrows 16, facilitating communications between devices which are connected to those other ISP's with other devices over the Internet, which may include the devices 12(n) connected to ISP 11.

The devices 13 which devices 12(m) access and communicate with may also be any of a number of types of devices, including personal computers, computer workstations, and the like, and also including mini-and mainframe computers, mass storage systems, compute servers, local area networks ("LAN's") and wide area networks ("WAN's") including such devices and numerous other types of devices which may be connected directly or indirectly to the networks. In connection with the invention, at least one of the devices will include at least one private network, identified as virtual private network 15, which may be in the form of a LAN or WAN. The virtual private network 15 may comprise any of the devices 12(m') (m'≠m) (thereby connecting to the Internet 14

through an ISP) or 13 (thereby connecting directly to the Internet 14); in the illustrative embodiment described herein, the virtual private network 15 will be assumed to comprise a device 13. The virtual private network 15 itself includes a plurality of devices, identified herein as a firewall 30, a plurality of servers 31(1) through 31(S) (generally identified by reference numeral 31(s)) and a nameserver 32, all interconnected by a communication link 33. The firewall 30 and servers 31(s) may be similar to any of the various types of devices 12(m) and 13 described herein, and thus may include, for example, personal computers, computer workstations, and the like, and also including mini-and mainframe computers, mass storage systems, compute servers, local area networks ("LAN's") and wide area networks ("WAN's") including such devices and numerous other types of devices which may be connected directly or indirectly to the networks.

As noted above, the devices, including devices 12(m) and devices 13, communicate by transferring message packets over the Internet. The devices 12(m) and 13 can transfer information in a "peer-to-peer" manner, in a "client-server" manner, or both. Generally, in a "peer-to-peer" message packet transfer, a device merely transfers information in one or more message packets to another device. On the other hand, in a "client-server" manner, a device, operating as a client, can transfer a message packet to another device, operating as a server to for example, initiate service by the other device. A number of types of such services will be appreciated by those skilled in the art, including, for example, the retrieval of information from the other device, to enable the other device to perform processing operations, and the like. If the server is to provide information to the client, it (that is, the server) may generally be referred to as a storage server. On the other hand, if the server is to perform processing operations at the request of the client, it (that is, the server) may generally be referred to as a compute server. Other types of servers, for performing other types of services and operations at the request of clients, will be appreciated by those skilled in the art.

In a client/server arrangement, device 12(m) requiring service by, for example, a device 13, generates one or more request message packets requesting the required service, for transfer to the device 13. The request message packet includes the Internet address of the device 13 that is, as the destination device, to receive the message packet and perform the service. The device 12(m)

transfers the request message packet(s) to the ISP 11. The ISP 11, in turn, will transfer the message packet over the Internet to the device 13. If the device 13 is in the form of a WAN or LAN, the WAN or LAN will receive the message packet(s) and direct it (them) to a specific device connected therein which is to provide the requested service.

In any case, after the device 13 which is to provide the requested service receives the request message packet (s), it will process the request. If the device 12(m) which generated the request message packet(s), or its operator, has the required permissions to request the service from the device 13 which generated the request message packet, if the requested service is to initiate the transfer of information from the device 13 as a storage server to the device 12(m) as client, the device 13 will generate one or more response message packets including the requested information, and transmit the packet(s) over the Internet 14 to the ISP 11. The ISP 11, in turn, will transfer the message packet(s) to the device 12(m). On the other hand, if the requested service is to initiate processing by the device 13 as a compute server, the device 13 will perform the requested computation service(s). In addition, if the device 13 is to return processed data generated during the computations to the device 12(m) as client, the device 13 will generate one or more response message packet(s) including the processed data and transmit the packet(s) over the Internet 14 to the ISP 11. The ISP 11, in turn, will transfer the message packet(s) to the device 12(m). Corresponding operations may be performed by the devices 12(m) and 13, ISP 11 and Internet 14 in connection with other types of services which may be provided by the server devices 13.

As noted above, each message packet that is generated by devices 12(m) and 13 for transmission over the Internet 14 includes a destination address, which the switching nodes use to route the respective message packet to the appropriate destination device. Addresses over the Internet are in the form of an "n"-bit integer (where "n" currently may be thirty two or 128). To relieve, in particular, an operator of a device 12(m) of the necessity of remembering specific integer Internet addresses and providing them to the device 12(m) to initiate generation of a message packet for transmission over the Internet, the Internet provides a second addressing mechanism which is more easily utilized by human operators of the respective devices. In that addressing mechanism,

Internet domains, such as LAN's, Internet service providers ("ISP's") and the like which are connected in the Internet, are identified by relatively human-readable names. To accommodate human-readable domain names, ISP 11 is associated with a nameserver 17 (which may also be referred to as a DNS servers), which can resolve the human-readable domain names to provide the appropriate Internet address for the destination referred to in the respective human-readable name. Generally, the nameserver may be part of or connected directly to the ISP 11, as shown in FIG. 1, or it may be a particular device which is accessible through the ISP over the Internet. In any case, as noted above, when the device 12(m) logs on to the ISP 11 during a communications session, the ISP 11 will assign various Internet protocol ("IP") parameters which the device 12(m) is to use during the communications session, which will be stored in the Internet parameter store 25. These IP parameters include such information as

(a) an Internet address for the device 12(m) which will identify the device 12(m) during the communications session, and

(b) the identification of a nameserver 17 that the device 12(m) is to use during the communications session.

The device 12(m), when it generates message packets for transfer, will include its Internet address (item (a) above) as the source address. The device(s)13 which receives the respective message packets can use the source address from message packets received from the device 12(m) in message packets which they (that is, device(s) 13) generate for transmission to the device 12(m), thereby to enable the Internet to route the message packets generated by the respective device 13 to the device 12(m). If the device 12(m) is to access the nameserver 17 over the Internet 14, the nameserver identification provided by the ISP 11 (item (b) above) will be in the form of an integer Internet address which will allow the device 12(m) to generate messages to the nameserver 17 requesting resolution of human-readable Internet addresses into integer Internet addresses. The ISP 11 may also assign other IP parameters to the device 12(m) when it logs on to the ISP 11, including, for example, the identification of a connection to the Internet 14 that is to be used for messages transmitted by the

device 12(m), particularly if the ISP 11 has multiple gateways. Generally, the device 12(m) will store the Internet parameters in the Internet parameter store 25 for use during the communications session.

When an operator operating device 12(m) wishes to enable the device 12(m) to transmit a message packet to a device 13, he or she provides the Internet address for the device 13 to the device 12(m), through the operator interface 20, and information, or the identification of information maintained by the device 12(m) that is to be transmitted in the message. The operator interface 20, in turn, will enable the packet generator 22 to the required packets for transmission through the ISP 11 over the Internet 11. If

(i) the operator has provided the integer Internet address, or

(ii) the operator has provided the human-readable Internet address, but the packet generator 22 already has the integer Internet address which corresponds to the human-readable Internet address provided by the operator,

the packet generator 22 may generate the packets directly upon being enabled by the operator interface 20, and provide them to the network interface 21 for transmission to the ISP 11.

However, if the operator has provided the human-readable Internet address for the device 13 to which the packets are to be transferred, and if the packet generator 22 does not already have the corresponding integer Internet address therefor, the packet generator 22 will enable the network address to be obtained from the nameserver 17 identified in the IP parameter store 25. In that operation, the packet generator 22 will initially contact nameserver 17 to attempt to obtain the appropriate integer Internet address from the nameserver 17. In these operations, the device 12(m) will generate appropriate message packets for transmission to the nameserver 17, using the nameserver's integer Internet address as provided by the ISP 11 when it (that is, the device 12(m)) logs on at the beginning of the communications session. In any case, if the nameserver 17 has or can obtain the integer Internet address for the human-readable name, it (that is, the nameserver 17) will

provide the integer Internet address to the device 12(m). The integer Internet address will be received by the packet generator 22 through the network interface 21 and packet receiver and processor 23. After the packet generator 22 receives the integer Internet address, it can generate the necessary message packets for transmission to the device 13 through the network interface 21 and ISP 11.

As noted above, one of the devices 13 connected to the Internet 14 is virtual private network 15, the virtual private network 15 including a firewall 30, a plurality of devices identified as servers 31(s), and a nameserver 32 interconnected by a communication link 33. The servers 31(s), firewall 30 and nameserver 32 can, as devices connected in a LAN or WAN, transfer information in the form of message packets thereamong. Since the firewall 30 is connected to the Internet 14 and can receive message packets thereover it has an Internet address. In addition, at least the servers 31(s) which can be accessed over the Internet also have respective Internet addresses, and in that connection the nameserver 32 serves to resolve human-readable Internet addresses for servers 31(s) internal to the virtual private network 15 to respective integer Internet addresses.

Generally, the virtual private network 15 is maintained by a company, governmental agency, organization or the like, which desires to allow the servers 31(s) to access other devices outside of the virtual private network 15 and transfer information thereto over the Internet 14, but which also desires to limit access to the servers 31(s) by devices 12(m) and other devices over the Internet 14 in a controlled manner. The firewall 30 serves to control access by devices external to the virtual private network 15 to servers 31(s) within the virtual private network 15. In that operation, the firewall 30 also connects to the Internet 14, receives message packets therefrom for transfer to a server 31(s). If the message packet indicates that the source of the message packet is requesting access to the particular server 31(s), and if the source is authorized to access the server 31(s), the firewall 30 will forward the message packet over the communication link 33 to the server 31(s). On the other hand if the source is not authorized to access the server 31(s), the firewall 30 will not forward the message packet to the server 31(s), and may, instead, transmit a response message packet to the source device indicating that the source was not authorized to access the server 31(s). The

firewall may be similar to other devices 31(s) in the virtual private network 15, with the addition of one or more connections to the Internet, which are generally identified by reference numeral 43.

Communications between devices external to the virtual private network 15, such as device 12(m), and a device, such as a server 31(s), inside the virtual private network 15, may be maintained over a secure tunnel between the firewall 30 and the external device as described above to maintain the information transferred therebetween secret while being transferred over the Internet 14 and through the ISP 11. A secure tunnel between device 12(m) and virtual private network 15 is represented in FIG. 1 by logical connections identified by reference numerals 40, 42, and 44; it will be appreciated that the logical connection 42 comprises one of the logical connections 41 between ISP 11 and Internet 14, and logical connection 44 comprises one of the logical connections 43 between the Internet 14 and the firewall 30.

Establishment of a secure tunnel can be initiated by device 12(m) external to the virtual private network 15. In that operation, the device 12(m), in response to a request from its operator, generates a message packet for transfer through the ISP 11 and Internet 14 to the firewall 30 requesting establishment of a secure tunnel between the device 12(m) and firewall 30. The message packet may be directed to a predetermined integer Internet address associated with the firewall 30 which is reserved for secure tunnel establishment requests, and which is known to and provided to the device 12(m) by the nameserver 17. If the device 12(m) is authorized to access a server 31(s) in the virtual private network 15, the client 12(m) and firewall 30 engage in a dialog, comprising one or more message packets transferred therebetween over the Internet 14. During the dialog, the firewall 30 may provide the device 12(m) with the identification of a decryption algorithm and associated decryption key which the device 12(m) is to use in decrypting the encrypted portions of message packets which the virtual private network transmits to the device 12(m). In addition, the firewall 30 may also provide the device 12(m) with the identification of an encryption algorithm and associated encryption key which the device 12(m) is to use in encrypting the portions of message packets which the device 12(m) transmits to the virtual private network 15 which are to be encrypted; alternatively, the device 12(m) can provide the identification of the encryption algorithm

and key that it (that is device 12(m)) will use to the firewall 30 during the dialog. The device 12(m) can store in its IP parameter store 25 information concerning the secure tunnel, including information associating the identification of the firewall 30 and the identifications of the encryption and decryption algorithms and associated keys for message packets to be transferred over the secure tunnel.

Thereafter, the device 12(m) and firewall 30 can transfer message packets over the secure tunnel. The device 12(m), in generating message packets for transfer over the secure tunnel, makes use of the secure packet processor 26 to encrypt the portions of the message packets which are to be encrypted prior to transmission by the network interface 21 to the ISP 11 for transfer over the Internet 14 to the firewall 30, and to decrypt the encrypted portions of the message packets received by the device 12(m) which are encrypted. In particular, after the packet generator 22 generates a message packet for transmission to the firewall 30 over the secure tunnel, it will provide the message packet to the secure packet processor 26. The secure packet processor 26, in turn, encrypts the portions of the message packet that are to be encrypted, using the encryption algorithm and key. After the firewall 30 receives a message packet from the device 12(m) over the secure tunnel, it will decrypt it and, if the intended recipient of the message packet is another device, such as a server 31(s), in the virtual private network 14, it (that is, the firewall 30) will transfer the message packet to that other device over the communication link 33.

For a message packet that is to be transferred by a device, such as a server 31(s), in the virtual private network 15 to the device 12(m) over the secure tunnel, the firewall 30 will receive such to the message packet over the communication link 33 and encrypt the message packet for transfer over the Internet 14 to the ISP 11. The ISP 11, in turn, forwards the message packet to the device 12(m), in particular to its network interface 21. The network interface 21 provides the message packet to the secure packet processor 26, which decrypts the encrypted portions of the message packet, using the decryption algorithm and key.

A problem arises in connection with accesses by a device, such as device 12(m), which is external to the virtual private network 15, and a device, such as a server 31(s), which is external to the firewall, namely, that nameserver 17 is not provided with integer Internet addresses for servers 31(s) and other devices which are in the virtual private network 15, except for integer Internet addresses associated with the firewall 30. Thus, the device 12(m), after the operator has entered the human-readable Internet address, will not be able to obtain the integer Internet address of the server 31(s) which is to be accessed from that nameserver 17.

To accommodate this problem, when the device 12(m) and firewall 30 cooperate to establish a secure tunnel therebetween, in addition to possibly providing the device 12(m) with the identifications of the encryption and decryption algorithms and keys which are to be used in connection with the message packets transferred over the secure tunnel, the firewall 30 also provides the device 12(m) with the identification of a nameserver, such as nameserver 32, in the virtual private network 15 which the device 12(m) can access to obtain the appropriate integer Internet addresses for the human-readable Internet addresses which may be provided by the operator of device 12(m). The identification of nameserver 32 is also stored in the IP parameter store 25, along with the identification of nameserver 17 which was provided by the ISP 11 when the device 12(m) logged on to the ISP 11 at the beginning of a communications session. Thus, when the device 12(m) is to transmit a message packet to a device, such as a server 31(s) in the virtual private network 14 using a human-readable Internet address provided by, for example, an operator, the device 12(m) will initially access the nameserver 17, as described above, to attempt to obtain the integer Internet address associated with the human-readable Internet address. Since nameserver 17 is outside of the virtual private network 15 and will not have the information requested by the device 12(m), it will send a response message packet so indicating. The device 12(m) will thereafter generate a request message packet for transmission to the nameserver 32 through the firewall 30 and over the secure tunnel. If the nameserver 32 has an integer Internet address associated with the human-readable Internet address in the request message packet provided by the device 12(m), it will provide the integer Internet address in a manner that is generally similar to that described above in connection

with nameserver 18, except that the integer Internet address will be provided by the nameserver 32 in a message packet directed to the firewall 30, and the firewall 30 will thereafter transmit the message packet over the secure tunnel to the device 12(m). In the message packet transmitted by the firewall 30, it will be appreciated that the integer Internet address in the message packet will be in the data portion of the message packet transferred over the secure tunnel and, accordingly, will be in encrypted form. The message packet will be processed by the device 12(m) in a manner similar to that described above in connection with other message packets received by it over the secure tunnel, that is, the message packet will be decrypted by the secure packet processor 26 prior to being provided to the packet receiver and processor 23 for processing. The integer Internet address for the server 31(s) can be cached in an access control list ("ACL") in the IP parameter store 25, along with the association of the human-readable Internet address thereto, an indication that the server 31(s) associated with that human-readable Internet address is to be accessed through the firewall 30 of the virtual private network 15, and the identifications of the encryption and decryption algorithms and keys to be used for encrypting and decrypting the appropriate portions of the message packets transmitted to server 31(s) and received from server 31(s).

It will be appreciated that, if the nameserver 32, in response to a message packet from the device 12(m) requesting the nameserver 32 to provide an integer Internet address for a human-readable Internet address provided by the device 12(m), if the nameserver 32 does not have an association between the human-readable Internet address and an integer Internet address, the nameserver 32 can provide a response message packet so indicating. If the device 12(m) has identification of other nameservers, such as may be associated with other virtual private networks (not shown), to which it (that is, device 12(m)) may have access, then the device 12(m) can attempt to access the other nameservers in a similar manner as described above. If the device 12(m) is unable to obtain an integer Internet address associated with the human-readable Internet address from any of the nameservers to which it has access, and which generally will be identified in its IP parameter store 25, it will generally be unable to access a device having the human-readable Internet address, and may so notify its operator or program which requested the access.

With this background, operations performed by the device 12(m) and virtual private network 15 in connection with the invention will be described in detail. Generally, operations proceed in two phases. In the first phase, the device 12(m) and virtual private network 15 cooperate to establish a secure tunnel through the Internet 14. In that first phase, the virtual private network 15, in particular the firewall 30 provide the identification of a nameserver 32, and may also provide the encryption and decryption algorithm and key information, as described above. In the second phase, after the secure tunnel has been established, the device 12(m) can use the information provided during the first phase in connection with generating and transferring message packets to one or more servers 31(s) in the virtual private network 15, in the process obtaining resolution human-readable Internet addresses to integer Internet addresses as necessary from the nameserver 32 that was identified by the firewall 30 during the first phase.

Thus, in the first (secure tunnel establishment) phase, the device 12(m) initially generates a message packet requesting establishment of a secure tunnel for transfer to the firewall 30. The message packet will include an integer Internet address for the firewall (which may have been provided by the device's operator or a program being processed by the device 12(m) or have been provided by a the nameserver 17 after a human-readable Internet address was provided by the operator or a program), and which, in particular, is to enable the firewall 30 to establish secure tunnels therewith. If the firewall 30 accepts the secure tunnel establishment request, and if the firewall 30 provides the encryption and decryption algorithms and keys as noted above, it (that is, the firewall) will generate a response message packet for transmission to the device 12(m) that identifies the encryption and decryption algorithms and keys; as noted above, this response message packet will not be encrypted. When the device 12(m) receives the response message, the identifications of the encryption and decryption algorithms and keys will be stored in the IP parameter store 25.

At some point later in the first phase, the firewall 30 will also generate a message packet for transmission to the device 12(m) that includes the integer Internet address of the nameserver 32. For this message packet, the portion of the message packet that contains the integer Internet address of

the nameserver 32 will be encrypted, using encryption algorithm and key that can be decrypted using the decryption algorithm and key provided in the response message packet described above. This message will generally have a structure

"<IIA(FW),IIA(DEV12(m))><SEC_TUN>

<ENCR<<IIA(FW),IIA(DEV_12(m))><DNS_ADRS:IIA(NS_32)>>>"

where

(i) "IIA(FW)" represents the source address, that is, integer Internet address of the firewall 30,

(ii) "IIA(DEV_12(m))" represents the destination address, that is, the integer Internet address of the device 12(m),

(iii) "DNS_ADRS:IIA(NS) indicates that "IIA(NS_32)" represents the integer Internet address of the nameserver 32, the nameserver which the device 12(m) is authorized to use, and

(iv) "ENCR<....>" indicates that the information between brackets "<" and >" is encrypted.

The initial portion of the message "<IIA(FW),IIA(DEV_12(m))>" forms at least part of the header portion of the message, and "<ENCR<<IIA(FW),IIA(DEV_12(m))><IIA(NS)>>>" represents at least part of the data portion of the message. The "<SEC_TUN>" represents an indicator in the header indicating that the message is being transferred over the secure tunnel, thereby indicating that the data portion of the message contains encrypted information.

After the device 12(m) receives the message from the firewall 30 as described above, since the message packet contains the <SEC_TUN> indicator, its network interface 21 will transfer the encrypted portion "<ENCR<<IIA(FW),IIA(DEV_12(m))><DNS_ADRS:IIA(NS_32)>>>" to the secure packet processor 26 for processing. The secure packet processor will decrypt the encrypted portion, determine that the portion "IIA(NS_32)" is the integer Internet address of a nameserver, in

particular nameserver 32, that the device 12(m) is authorized to use, and store that address in the IP parameter store 25, along with an indication that message packets thereto are to be transferred to the firewall 30 and that data in the message packets is to be encrypted using the encryption algorithm and key previously provided by the firewall 30. It will be appreciated that, since the integer Internet address of nameserver 32 is transferred from the firewall to the device 12(m) in encrypted form, it will be maintained in confidence even if the packet is intercepted by a third party.

Depending on the particular protocol used to establish the secure tunnel, the firewall 30 and device 12(m) may also exchange message packets containing other information than that described above.

As noted above, in the second phase, after the secure tunnel has been established, the device 12(m) can use the information provided during the first phase in connection with generating and transferring message packets to one or more of the servers 31(s) in the virtual private network 15. In those operations, if the operator of device 12(m), or a program being processed by device 12(m), wishes to have device 12(m) transmit a message packet to a server 31(s) in the virtual private network 15, if the operator, through the operator interface 20, or the program provides a human-readable Internet address, the device 12(m), in particular the packet generator 22, will initially determine whether the IP parameter store 25 has cached therein an integer Internet address that is associated with the human-readable Internet address. If not, the packet generator 22 will generate a request message packet for transfer to the nameserver 17 requesting it to provide the integer Internet address associated with the human-readable Internet address. If the nameserver 17 has an integer Internet address associated with the human-readable Internet address, it will provide the integer Internet address to the device 12(m). It will be appreciated that this may occur if the human-readable Internet address in the request message packet has been associated with a device 13 external to the virtual private network 15, as well as with a server 32(s) in the virtual private network 15. Thereafter, the device 12(m) can use the integer Internet address to generate message packets for transfer over the Internet as described above.

Assuming, on the other hand, that the nameserver 17 does not have a integer Internet address associated with the human-readable Internet address, it (that is, the nameserver 17) will provide a response message packet so indicating to the device 12(m). Thereafter, the packet generator 22 of device 12(m) will generate a request message packet for transmission to the next nameserver identified in its IP parameter store 25 requesting that nameserver to provide the integer Internet address associated with the human-readable Internet address. If that next nameserver is nameserver 32, the packet generator 22 will provide the message packet to the secure packet processor 26 for processing. The secure packet processor 26, in turn, will generate a request message packet for transfer over the secure tunnel to the firewall 30. This message will generally have a structure

"<IIA(DEV_12(m)),IIA(FW)><SEC_TUN>

<ENCR<<IIA(DEV_12(m)),IIA(NS_32))><IIA_REQ>>>"

where

(i) "IIA(DEV_12(m))" represents the source address, that is, integer Internet address of the device 12(m)

(ii) "IIA(FW)" represents the destination address, that is, the integer Internet address of the firewall 30

(iii) "IIA(NS_32)" represents the address of the nameserver 32

(iii) "<<IIA(DEV_12(m)),IIA(NS_32))><IIA_REQ>>" represents the request message packet generated by the packet generator 22, where "<IIA(DEV_12(m)),IIA(NS_32)> represents the header portion of the request message packet, and "<IIA_REQ>" represents the data portion of the request message packet,

(iv) "ENCR<....>" indicates that the information between brackets "<" and >" is encrypted, and

(v) "<SEC_TUN>" represents an indicator in the header portion of the message packet generated by the secure packet generator 26 indicating that the message is being transferred over the secure tunnel, thereby indicating that the data portion of the message contains encrypted information.

When the firewall 30 receives the request message packet generated by the secure packet processor 26, it will decrypt the encrypted portion of the message packet to obtain <<IIA(DEV_12(m)),IIA(NS_32))><IIA_REQ>>" represents the request message packet as generated by the packet generator 22. After obtaining the request message packet, the firewall 30 will transmit it over the communication link 33 to the nameserver 32. In that process, depending on the protocol for transmission of message packets over the communication link 33, the firewall 30 may need to modify the request message packet to conform to the protocol of communication link 33.

After the nameserver 32 receives the request message packet, it will process it to determine whether it has an integer Internet address associated with the human-readable Internet address provided in the request message packet. If the nameserver determines that it has such an integer Internet address, it will generate a response message packet including the integer Internet address for transmission to the firewall. Generally, the response message packet will have a structure:

<<IIA(NS_32),IIA(DEV_12(m))><IIA_RESP>>

where

(i) "IIA(NS_32)" represents the source address, that is, integer Internet address of the nameserver 32,

(ii) "IIA(DEV_12(m))" represents the destination address, that is, integer Internet address of the device 12(m), and

(iii) "IIA_RESP" represents the integer Internet address associated with the human-readable Internet address.

After the firewall 30 receives the response message packet, since communications with device 12(m) are over the secure tunnel therebetween, it (that is, the firewall 30) will encrypt the response message packet received from the nameserver 32 and generate a message packet for transmission to the device 12(m) including the encrypted response message packet. Generally, the message packet generated by the firewall 30 has the structure:

"<IIA(FW),IIA(DEV12(m))><SEC_TUN>

<ENCR<<IIA(NS_32),IIA(DEV_12(m))><IIA_RESP>>>"

where

(i) "IIA(FW)" represents the source address, that is, integer Internet address of the firewall 30,

(ii) "IIA(DEV_12(m))" represents the destination address, that is, the integer Internet address of the device 12(m),

(iii) "SEC_TUN" represents an indicator in the header portion of the message packet generated by the secure packet generator 26 indicating that the message is being transferred over the secure tunnel, thereby indicating that the data portion of the message contains encrypted information, and

(iv) "ENCR<....>" indicates that the information between brackets "<" and >" (which constitutes the response message packet received from the nameserver 32) is encrypted.

In addition, depending on the protocol for transmission of message packets over the communication link 33, the firewall 30 may need to process and/or modify the message packet to conform to the protocol of Internet 14.

When the device 12(m) receives the message packet from the firewall 30, it (that is, the message packet) will be provided to the secure packet processor 26. The secure packet processor 26, in turn, will decrypt the encrypted portion of the message packet to obtain the integer Internet address associated with the human-readable Internet address, and load that information in the IP parameter store 25. Thereafter, the device can use that integer Internet address in generating message packets for transmission to the server 31(s) which is associated with the human-readable Internet address.

It will be appreciated that, if the nameserver 32 does not have an integer Internet address associated with the human-readable Internet address provided by the device 12(m) in the request message packet, it (that is, nameserver 32) can so indicate in the response message packet generated thereby. The firewall 30 will, in response to the response message packet provided by the nameserver 32, also generate a message packet for transmission to the device 12(m), the message packet including an encrypted portion comprising the response message packet generated by the nameserver 32. After the device 12(m) receives the message packet, the encrypted portion will be decrypted by the secure packet processor 26, which, in turn, will notify the packet generator 22 that the nameserver 32 does not have an integer Internet address associated with the human-readable Internet address. Thereafter, if the IP parameter store 25 contains the identification of another nameserver, the packet generator 22 of device 12(m) will generate a request message packet for transmission to the next nameserver identified in its IP parameter store 25 requesting that nameserver to provide the integer Internet address associated with the human-readable Internet address. On the other hand, if the IP parameter store 25 does not contain the identification of another nameserver, the packet generator 22 can notify the operator interface 20 or program that it is will be unable to generate a message packet for transmission to a device associated with the human-readable Internet address provided thereby.

An embodiment of the invention can provide a number of advantages. For example, it can provide a system for easing communications between devices connected to a public network such as the Internet 14, and devices connected to private networks such as virtual private network 15, by facilitating resolution

of human-readable addresses to network addresses by a nameservers connected to the private networks over a secure tunnel.

It will be appreciated that numerous modifications may be made to the arrangement described above in connection with FIG. 1. For example, although the network 10 has been described such that the identification of the encryption and decryption algorithms and keys are exchanged by the device 12(m) and firewall 30 during the dialog during which the secure tunnel is established, it will be appreciated that that information may be provided by the device 12(m) and firewall 30 separately from the establishment of a secure tunnel therebetween.

In addition, although an embodiment of the invention has been described in connection with the Internet, it will be appreciated that an embodiment of the invention can be used in connection with any network. Further, although an embodiment has been described in connection with a network which provides for human-readable network addresses, it will be appreciated that an embodiment can be used in connection with any network which provides for any form of secondary or informal network address arrangements.

It will be appreciated that a system in accordance with the invention can be constructed in whole or in part from special purpose hardware or a general purpose computer system, or any combination thereof, any portion of which may be controlled by a suitable program. Any program may in whole or in part comprise part of or be stored on the system in a conventional manner, or it may in whole or in part be provided in to the system over a network or other mechanism for transferring information in a conventional manner. Thus, such a computer program can form a product operable, when run on a computer, to provide the required functionality of an embodiment of the invention. The computer program product can be provided on a carrier medium, for example, a computer readable medium such as, for example, a memory, disc or other storage medium, or a transmission medium such as a telecommunications channel providing, for example, electrical, optical, wireless or other transmission. In addition, it will be appreciated that the system may be operated and/or otherwise controlled by means of information provided by an operator using operator input elements (not shown) which may be connected directly to the system or which may transfer the information to the system over a network or other mechanism for transferring information in a conventional manner.

The foregoing description has been limited to a specific embodiment of this invention. It will be apparent, however, that various variations and modifications may be made to the invention, with the attainment of some or all of the advantages of the invention.

CLAIMS

1. A system comprising a virtual private network and an external device which communicate over a digital network,

the virtual private network having a firewall, at least one internal device and a nameserver each having a network address, the internal device also having a secondary address, the nameserver being configured to provide an association between the secondary address and the network address,

the firewall, in response to a request from the external device to establish a connection therebetween, being configured to provide the external device with the network address of the nameserver, and

the external device, in response to a request requesting access to the internal device including the internal device's secondary address, being configured to generate a network address request message for transmission over the connection to the firewall requesting resolution of the network address associated with the secondary address, the firewall being configured to provide the address resolution request to the nameserver, the nameserver being configured to provide the network address associated with the secondary address, the firewall in turn being further configured to provide the network address in a network address response message for transmission over the connection to the external device.

2. A system according to claim 1, wherein the external device is further configured to use the network address provided in the network address response message in generating at least one message for transmission to the internal device.

3. A system according to claim 1 or claim 2, wherein the external device is configured to connect to the network through a network service provider.

4. A system according to claim 3, wherein the external device is configured to establish a communications session with the network service provider, the network service provider providing the external device with the identification of a further nameserver, the further nameserver being configured to provide an association between a secondary address and a network address for at least one device.

5. A system according to any preceding claim, wherein the external device is configured to maintain a list of nameservers which have been identified to said external device, the external device being configured to interrogate successive ones of the nameservers in the list in response to a request requesting access to another device, said request including a secondary address for said other device, until said external device receives a network address, in each interrogation the external device being configured to generate a said network address request message for transmission over the network for response by one of said nameservers in said list and to receive a network address response message therefrom.

6. A system according to any preceding claim, wherein the connection between the external device and the firewall is a secure tunnel, in which at least some portion of messages transferred between the external device and the firewall is encrypted.

7. A method of operating a system comprising a virtual private network and an external device interconnected by a digital network, the virtual private network having a firewall, at least one internal device and a nameserver each having a network address, the internal device also having a

secondary address, the nameserver being configured to provide an association between the secondary address and the network address, the method comprising the steps of:

A. enabling the firewall, in response to a request from the external device to establish a connection therebetween, provide the external device with the network address of the nameserver; and

B. enabling

(i) the external device, in response to a request requesting access to the internal device including the internal device's secondary address, to generate a network address request message for transmission over the connection to the firewall requesting resolution of the network address associated with the secondary address,

(ii) the firewall to provide the address resolution request to the nameserver,

(iii) the nameserver to provide the network address associated with the secondary address, and

(iv) the firewall to provide the network address in a network address response message for transmission over the connection to the external device.

8. A method according to claim 7, wherein the external device is further enabled to use the network address provided in the network address response message in generating at least one message for transmission to the internal device.

9. A method according to claim 7 or claim 8, wherein the external device is enabled to connect to the network through a network service provider.

10. A method according to claim 9, wherein the external device is enabled to establish a communications session with the network service provider, the network service provider being enabled to provide the external device with the identification of a further nameserver, the further nameserver being enabled to provide an association between a secondary address and a network address for at least one device.

11. A method according to any one of claims 7 to 10, wherein the external device is enabled to maintain a list of nameservers which have been identified to said external device, the external device being enabled to interrogate successive ones of the nameservers in the list in response to a request requesting access to another device, said request including a secondary address for said other device, until said external device receives a network address, in each interrogation the external device being enabled to generate a said network address request message for transmission over the network for response by one of said nameservers in said list and to receive a network address response message therefrom.

12. A method according to any one of claims 7 to 10, wherein the connection between the external device and the firewall is a secure tunnel, in which at least some portion of messages transferred between the external device and the firewall is encrypted.

13. A computer program product for use in connection with a virtual private network and an external device interconnected by a digital network, the virtual private network having a firewall, at least one internal device and a nameserver each having a network address, the internal device also having a secondary address, the nameserver being configured to provide an association between the secondary

address and the network address, the computer program product comprising :

A. a nameserver identification code module configured to enable the firewall, in response to a request from the external device to establish a connection therebetween, to provide the external device with the network address of the nameserver,

B. a network address request message generating code module for enabling the external device, in response to a request requesting access to the internal device including the internal device's secondary address, to generate a network address request message for transmission over the connection to the firewall requesting resolution of the network address associated with the secondary address,

C an address resolution request forwarding module for enabling the firewall to provide the address resolution request to the nameserver,

D. a nameserver control module for enabling the nameserver to provide the network address associated with the secondary address, and

E. a network address response message forwarding module for enabling the firewall to provide the network address in a network address response message for transmission over the connection to the external device.

14. A computer program product according to claim 13, further comprising a network address utilization module configured to enable the external device to use the network address provided in the network address response message in generating at least one message for transmission to the internal device.

15. A computer program product according to claim 13 or claim 14, further comprising a network service provider control module for enabling the external device to connect to the network through a network service provider.

16. A computer program product according to claim 15, wherein the network service provider control module includes a communications session establishment module for enabling the external device to a communications session with the network service provider and receive therefrom identification of a further nameserver.

17. A computer program product according to any one of claims 13 to 16, further including nameserver interrogation control module for enabling the external device to maintain a list of nameservers which have been identified to said external device, and to interrogate successive ones of the nameservers in the list in response to a request requesting access to another device, said request including a secondary address for said other device, until said external device receives a network address, in each interrogation the external device being enabled to generate a said network address request message for transmission over the network for response by one of said nameservers in said list and to receive a network address response message therefrom.

18. A computer program product according to any one of claims 13 to 16, wherein the connection between the external device and the firewall is a secure tunnel, in which at least some portion of messages transferred between the external device and the firewall is encrypted.

19. A computer program product according to any one of claims 13 to 18 on a carrier medium.

20. A computer program product according to claim 19, wherein the carrier medium is a computer readable medium.

21. A computer program product according to claim 19, wherein the carrier medium is a transmissions medium.

22. A system substantially as hereinbefore described with reference to the accompanying drawings.

23. A method substantially as hereinbefore described with reference to the accompanying drawings.

24. A computer program product substantially as hereinbefore described with reference to the accompanying drawings.

Office

34

INVESTOR IN PEOPLE

Application No: GB 9912200.4
Claims searched: All

Examiner: Gareth Griffiths
Date of search: 7 December 1999

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.Q): H4P (PPA, PPEB, PPEC, PPG)

Int Cl (Ed.6): H04L 12/22, 12/46, 12/66, 29/06

Other: Online Databases: WPI, EPODOC, JAPIO

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X, P	EP0887979 A2	(SUN MICROSYSTEMS) col.15 line 35 - col.17 line 24	1, 2, 5-8, 11-14, 17-21
A	EP0825748 A2	(AT&T) col.6 line 46 - col.11 line 40	
A, P	WO98/31124 A1	(HANSON) p.5 line 2 - p.6 line 25	

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Petitioner Apple Inc. - Exhibit 1002, p. 901

C19

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 12/66, H04Q 11/04

A1

(11) International Publication Number: **WO 98/43396**

(43) International Publication Date: 1 October 1998 (01.10.98)

(21) International Application Number: PCT/CA98/00197

(22) International Filing Date: 11 March 1998 (11.03.98)

(30) Priority Data:
08/821,145 20 March 1997 (20.03.97) US

(71) Applicant: NORTHERN TELECOM LIMITED [CA/CA]; World Trade Center of Montreal, 8th floor, 380 St. Antoine Street West, Montreal, Quebec H2Y 3Y4 (CA).

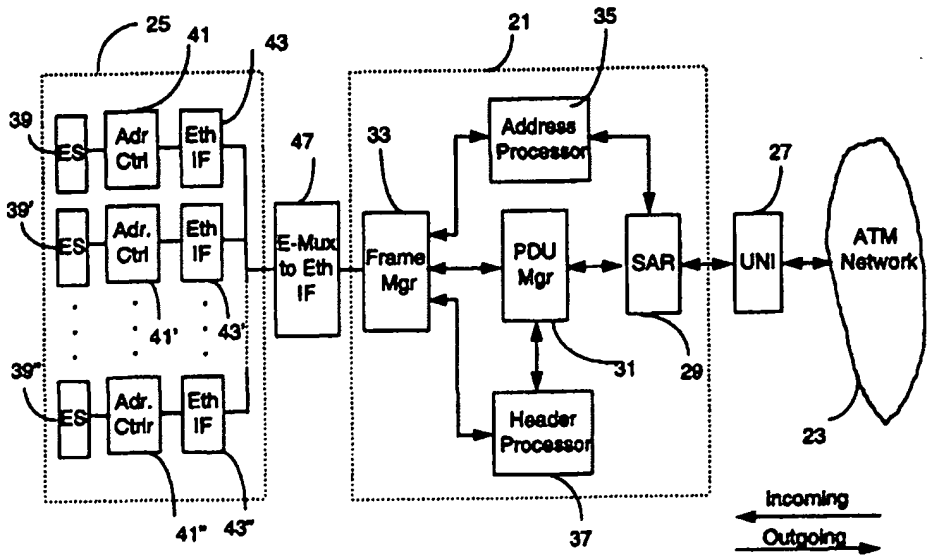
(72) Inventors: ALLAN, David, Ian; 852 Forest Street, Ottawa, Ontario K2B 5P9 (CA). CASEY, Liam, M.; 61 Aylmer Avenue, Ottawa, Ontario K1S 2X2 (CA). ROBERT, Andre, J.; 103 Sol Lane, R.R. #2, Woodlawn, Ontario K0A 3M0 (CA).

(74) Agent: DIACONESCU, Aprilia, U.; Northern Telecom Limited, Patent Dept., P.O. Box 3511, Station "C", Ottawa, Ontario K1Y 4H7 (CA).

(81) Designated States: AU, CA, JP, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: A MECHANISM FOR MULTIPLEXING ATM AAL5 VIRTUAL CIRCUITS OVER ETHERNET



(57) Abstract

The invention provides for an E-Mux and a method for encapsulating/segmenting ATM cells into/from an Ethernet frame at the boundary between an ATM and an Ethernet network. An Ethernet end-station on the E-Mux is addressed using multiple MAC level identifiers, which are dynamically assigned according to the ATM virtual circuits which terminate on that end station, and have only transitory significance on the Ethernet. A unique ATM OUI identifies the frames carrying ATM-traffic.

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : **H04L 9/00** | **A1**

(11) International Publication Number: **WO 99/1101**

(43) International Publication Date: 4 March 1999 (04.03.9

(21) International Application Number: PCT/US98/17198

(22) International Filing Date: 24 August 1998 (24.08.98)

(30) Priority Data:
08/917,341 26 August 1997 (26.08.97) US

(71) Applicant: V-ONE CORPORATION [US/US]; Suite 300, 20250 Century Boulevard, Germantown, MD 20874 (US).

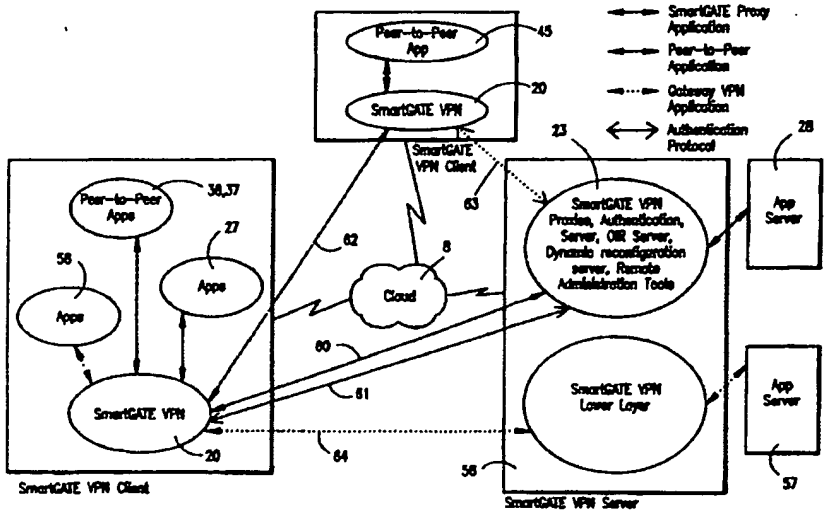
(72) Inventors: CHEN, James, F.; 12648 Tavilah Road, Potomac, MD 20854 (US). WANG, Jieh-Shan; 10903 Silent Wood Place, N. Potomac, MD 20878 (US). BROOK, Christopher, T.; 7308 Pomander Lane, Chevy Chase, MD 20815 (US). GARVEY, Francis; 2908 S. Buchanan Street, Arlington, VA 22206 (US).

(74) Agents: URCIA, Benjamin, E. et al.; Bacon & Thomas, PLLC, 4th floor, 625 Slaters Lane, Alexandria, VA 22314 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BI BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GI GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MX MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, T TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patei (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patei (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patei (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, I LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, C CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: MULTI-ACCESS VIRTUAL PRIVATE NETWORK



(57) Abstract

A virtual private network for communicating between a server and clients over an open network uses an applications level encryption and mutual authentication program (20) and at least one shim (50, 53) positioned above either the layers of a client computer to intercept function calls, communicate with the server and authenticate the parties to a communication and enable the parties to the communication to establish a common session key. Where the parties to the communication are peer-to-peer applications (36, 37, 45), the intercepted function calls, request for service, or data packets include the destination address of the peer application, which is supplied to the server so that the server can authenticate the peer and enable the peer to decrypt further direct peer-to-peer communications (62)

Petitioner Apple Inc. - Exhibit 1002, p. 903

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		

Petitioner Apple Inc. - Exhibit 1002, p. 904

MULTI-ACCESS VIRTUAL PRIVATE NETWORK

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates a system and method for allowing private communications over an open network, and in particular to a virtual private network which provides data encryption and mutual authentication services for both client/server and peer-to-peer applications at the applications, transport driver, and network driver levels.

2. Discussion of Related Art

A virtual private network (VPN) is a system for securing communications between computers over an open network such as the Internet. By securing communications between the computers, the computers are linked together as if they were on a private local area network (LAN), effectively extending the reach of the network to remote sites without the infrastructure costs of constructing a private network. As a result, physically separate LANs

can work together as if they were a single LAN, remote computers can be temporarily connected to the LAN for communications with mobile workers or telecommuting, and electronic commerce can be carried out without the risks inherent in using an open network.

In general, there are two approaches to virtual private networking, illustrated in Figs. 1A and 1B. The first is to use a dedicated server 1, which may also function as a gateway to a secured network 2, to provide encryption and authentication services for establishment of secured links 3 between the server 1 and multiple clients 4-6 over the open network 7, represented in Fig. 1A as a cloud, while the second is to permit private communications links 8 to be established between any two computers or computer systems 9-12 on network 7, as illustrated in Fig. 1B.

The advantages of a client/server arrangement such as the one shown in Fig. 1A are that the server can handle functions requiring the majority of the computing resources, increasing the number of potential clients, and that management of the network, including key management is centralized. The disadvantage of a client/server network of this type is that peer-to-peer communications links between applications on the client computers cannot utilize the security and management functions provided by the server, leaving such communications unprotected. On the

Petitioner Apple Inc. - Exhibit 1002, p. 906

other hand, the advantage of the direct peer-to-peer approach illustrated in Fig. 1B is that it permits secured links to be established between any computers capable of carrying out the required security functions, with the disadvantages being the cost of configuring each computer to carry-out encryption, authentication, and key management functions, and the lack of central control.

In both the client/server and peer-to-peer approaches, a virtual private network can in theory be based either on applications level technology or can operate at a lower level. Generally, however, peer-to-peer "tunneling" arrangements require modification of the lower layers of a computer's communications architecture, while client/server arrangements can use the applications level approach because less modification of the clients is required, and thus the two approaches are in practice mutually exclusive. The present invention, on the other hand, seeks to provide a virtual private network which utilizes a client/server approach, including centralized control of encryption, authentication, and key management functions, while at the same time enabling secured peer-to-peer communications between applications, by utilizing the server to provide authentication and session key generation functions for both client to server communications and peer-to-peer communications, providing a virtual private network capable of serving both as an extended intranet or wide area network (WAN), and as a commercial mass marketing network,

Petitioner Apple Inc. - Exhibit 1002, p. 907

with high level mutual authentication and encryption provided for all communications.

In order to completely integrate the two approaches and maximize the advantage of each approach, the invention maintains the applications level infrastructure of prior client server private networking arrangements, while adding shims to lower levels in order to accommodate a variety of peer-to-peer communications applications while utilizing the applications level infrastructure for authentication and session key generation purposes. This results in the synergistic effect that not only are existing peer-to-peer tunneling schemes and applications level client server security arrangements combined, but they are combined in a way which greatly reduces implementation costs

In order to understand the present invention, it is necessary to understand a few basic concepts about computer to computer communications, including the concepts of "layers" and communications protocols, and of mutual authentication and file encryption. Further information about layers and protocols can be found in numerous sources available on the Internet, a few of which are listed at the end of this section, while a detailed description of a mutual authentication and encryption system and method suitable for use in connection with the present invention can be found in U.S. Patent No. 5,602,918, which is incorporated herein by reference. In general, the basic

Petitioner Apple Inc. - Exhibit 1002, p. 908

communications protocols and architecture used by the present invention, as well as authentication, encryption, and key management schemes, are already well-known, and can be implemented as a matter of routine programming once the basic nature of the invention is understood. The changes made by the present invention to the conventional client server virtual private network may be thought of as, essentially, the addition of means, most conveniently implemented as shims, which add a secured mutual authentication and session key generation channel between the server and all parties to a communication, at all levels at which a communication can be carried out.

Having explained the key differences between the present invention and existing systems, the basic concepts of layers and so forth will now be briefly explained by way of background. First, the concept of "layers," "tiers," and "levels," which essential to an understanding of the invention, simply refers to libraries or sets of software routines for carrying out a group of related functions, and which can conveniently be shared or called on by different programs at a higher level to facilitate programming, avoiding duplication and maximizing computer resources. For example, the Windows NT device driver architecture is made up of three basic layers, the first of which is the Network Driver Interface Specification (NDIS 3.0) layer, the second of which is called the Transport Driver Interface (TDI) layer, and the third being the file

Petitioner Apple Inc. - Exhibit 1002, p. 909

systems. These layers are generically referred to as the network driver layer, the transport or transport driver layer, and the applications layer.

In the Windows NT architecture, the TDI layer formats data received from the various file systems or applications into packets or datagrams for transmission to a selected destination over the open network, while the NDIS layer controls the device drivers that send the data, packets, or IP datagrams, for example by converting the stream of data into a waveform suitable for transmission over a telephone line or a twisted pair cable of the type known as an Ethernet.

By providing layers in this manner, an applications software programmer can design an application program to supply data to the TDI layer without having to re-program any of the specific functions carried out by that layer, and all of the transmission, verification, and other functions required to send a message will be taken care of the TDI layer without further involvement by the applications software. In a sense, each "layer" simply accepts data from the higher layer and formats it by adding a header or converting the data in a manner which is content independent, with retrieval of the data simply involving reverse conversion or stripping of the headers, the receiving software receiving the data as if the intervening layers did not exist.

Petitioner Apple Inc. - Exhibit 1002, p. 910

In the case of Internet communications, the most commonly used set of software routines for the transport or TDI layer, which takes care of the data formatting and addressing, is the TCP/IP protocol, in which the transport control protocol (TCP) packages the data into datagrams and provides addressing, acknowledgements, and checksum functions, and the internet protocol (IP) further packages the TCP datagrams into packets by adding additional headers used in routing the packets to a destination address. Other transport protocols which can be included in the TDI layer include the user diagram protocol (UDP), the internet control message protocol (ICMP), and non-IP based protocols such as Netbeui or IPX.

Additional "protocols" are may be used at the applications level, although these protocols have nothing to do with the present invention except that they may be included in the applications programs served by the network. Common applications level protocols which utilize the TCP/IP protocol include hypertext transfer protocol (HTTP), simple mail transfer protocol (SMTP), and file transfer protocol (FTP), all of which operate at the layer above the transport layer.

Some applications are written to directly call upon the TCP functions. However, for most applications utilizing a graphical user interface conveniently rely on a set of software routines which are considered to operate

Petitioner Apple Inc. - Exhibit 1002, p. 911

above the TDI layer, and are known as sockets. Sockets serve as an interface between the TCP set of functions, or stack, and various applications, by providing libraries of routines which facilitate TCP function calls, so that the application simply has to refer to the socket library in order to carry out the appropriate function calls. For Windows applications, a commonly used non-proprietary socket is the Windows socket, known as Winsock, although sockets exist for other operating systems or platforms, and alternative sockets are also available for Windows, including the Winsock 2 socket currently under development.

In order to implement a virtual private network, the encryption and authentication functions must be carried out at one of the above "levels," for example by modifying the network drivers to encrypt the IP datagrams, by inserting authentication headers into the TCP/IP stacks, or by writing applications to perform these functions using the existing drivers. If possible, it is generally desirable to minimize modification of the existing levels by adding a layer to perform the desired functions, calling upon the services of the layer below, while utilizing the same function calls so that the higher layer also does not need to be modified. Such a layer is commonly referred to as a "shim."

As indicated above, the preferred approach to implementing client/server virtual private networks is to

Petitioner Apple Inc. - Exhibit 1002, p. 912

use an applications level security system to encrypt files to be transmitted, and to then utilize existing communications layers such as Winsock, or TCP/IP directly. This is the approach taken by the commercially available access control system known as SmartGATE™, developed by V-One Corp. of Germantown, Md., which provides both encryption and mutual authentication at the applications level utilizing a dedicated server known as an authentication server and authentication client software installed at the applications level on the client computers. A description of the manner in which encryption and mutual authentication is carried out may be found in the above-cited U.S. Patent No. 5,602,918. While the principles of the invention are applicable to other client/server based virtual private networks, SmartGATE™ is used as an example because it provides the most complete range of mutual authentication and encryption services currently available.

The present invention can be implemented using the existing SmartGATE™ system, but adds mutual authentication and encryption services to lower layers by intercepting function calls or data packets and, during initialization of a communications link, establishing separate channels between the party initiating the communication and the authentication server, and between the authentication server and the party which is to share in the communication, so as to mutually authenticate the parties

Petitioner Apple Inc. - Exhibit 1002, p. 913

with respect to the server, and so as to establish a session key which can be used for further direct communications between the parties.

A number of protocols exist which can be used, in total or in part, to implement the mutual authentication and encryption services at the lower layers, using the same basic authentication and encryption scheme currently implemented by SmartGATE™ at the applications level. These include, by way of example, the SOCKS protocol, which places a shim between the TDI or transport layer and the applications, and the commercially available program, known as SnareNet, which operates at the network driver level and can be directly utilized in connection with the present invention.

On the other hand, a network level implementation such as the SKIP protocol, which operates below the TDI layer to encrypt the datagrams, and which in its description explicitly precludes the generation of session keys (see the above cited U.S. Patent No. 5,602,918), is fundamentally different in concept than the present invention. Similarly, alternative implementations such as Point-to-Point Tunneling Protocol (PPTP) which involve modifying the TCP/IP stack and/or hardware to provide encryption, as opposed to inserting shims, are not utilized by the preferred embodiment of the present invention, although individual aspects of the protocol could perhaps

Petitioner Apple Inc. - Exhibit 1002, p. 914

be used, and the present system could be added to computers also configured to accept PPTP communications.

The SmartGATE™ system uses public key and DES encryption to provide two-way authentication and 56-bit encrypted communications between a server equipped with the SmartGATE program and client computers equipped with a separate program. Currently, SmartGATE™ operates at the highest level, or applications level, by using shared secret keys to generate a session key for use in further communications between the authentication server or gateway and the client program. Since the session key depends on the secret keys at the gateway and client sides of the communication, mutual authentication is established during generation of the session key, which can then be used to encrypt further communications.

When installed on a client system, the SmartGATE™ client software reads a request for communications by an applications program, such as a browser program, and then proceeds to establish its own communications link with the destination server to determine if the server is an authentication server. If it is not, control of communications is relinquished, but if it is, then the security program and the server carry out a challenge/response routine in order to generate the session key, and all further communications are encrypted by the security program. Although this program is placed between

Petitioner Apple Inc. - Exhibit 1002, p. 915

the Winsock layer and the applications, it does not function as a shim, however, because it only affects communications directed to the authentication server.

Having briefly summarized the concepts used by the present invention, including the concepts of layers, protocols, and shims, and having described a specific applications level security program which is to be modified according to the present invention by adding shims in a way which enables secured authentication and session key generation channels to be set up from the lower layers, it should now be possible to understand the nature of the invention, and in particular how it integrates the two approaches to virtual private networking in a way which greatly expands the concept and yet can easily be implemented. More details will be given below, but as a final observation in this background portion of the patent specification, it should be noted that while the overall concept of the invention is in a sense very simple, it is fundamentally at odds with present approaches. For example, the literature is replete with references to conflicts between VPN standards and implementations, as exemplified by the title of an article from LAN Times On-Line, 9/96, (http://www.wcmh.com/), which reads *Clash Over VPN Supremacy*. Even a cursory search of the available literature indicates that the amount of information and choices available to those wishing to set up a virtual private network is overwhelming. One can choose between

Petitioner Apple Inc. - Exhibit 1002, p. 916

Netscape Communications Secure Socket Layer, Open Market Inc.'s Secure HTTP, Microsoft's PPTP, among others. However, all of these approaches operate at a single level, and force a choice between establishing a network of the type shown in Fig. 1A and a network of the type shown in Fig. 1B. Only the present invention offer the advantages of both approaches, without the inflexibility of client/server arrangements or the costs of more distributed architectures.

For further information on the various competing VPN protocols and systems, see also *The Development of Network Security Technologies*, Internet Smartsec, 2/97 (http://www.smartsec.se), which compares SmartGATE™ to other application level security systems, including PPTP, SSL, and S-HTTP; *Point-To-Point Tunneling Protocol (PPTP) Frequently Asked Questions*, Microsoft Corp., date unknown, (http://www.microsoft.com), *Simple Key-Management for Internet Protocols (SKIP)*, Aziz *et al.*, date unknown, (http://skip.incog.com), and *SOCKS Protocol Version 5, RFC 1928*, Leech *et al.*, 3/96 (http://andrew2.andrew.cmu.edu) (this document describes a protocol involving a TDI shim). For more general information on security problems, Internet protocols, and sockets, see *Introduction to the Internet Protocols*, Charles L. Hedrick, Rutgers University, 1987 (http://oac3.hsc.uth.tmc.edu); *Windows Sockets - Where Necessity is the Mother of Reinvention*, Stardust

Petitioner Apple Inc. - Exhibit 1002, p. 917

Technologies, Inc., 1996, (http//www.stardust.com), and *Secure Internet Connections*, LAN Times, 6/17/96 (Ibid).

SUMMARY OF THE INVENTION

It is accordingly a principal objective of the invention to provide a client/server virtual private network which is capable not only of carrying out authenticated secure communications over an open network between an authentication server and clients, but also authenticated secure peer-to-peer communications.

It is also an objective the invention to provide a virtual private network that provides data encryption and mutual authentication for both client/server and peer-to-peer communications for different-types of applications, using both the applications level and lower levels of a communications hierarchy.

It is a further objective of the invention to provide a client/server virtual private network which can provide both client/server and peer-to-peer encryption and authentication services for any application sharing a specified socket or sockets, whether or not the application is recognized by the encryption and authentication program.

It is a still further objective of the invention to provide a client/server virtual private network which can

Petitioner Apple Inc. - Exhibit 1002, p. 918

provide encryption and authentication services at the applications level, transport driver interface level, and network interface level, without the need for modifying either the communication driver or network driver, or any sockets utilizing the communications driver interface.

It is yet another objective of the invention to provide a virtual private network which provides encryption and authentication services for peer-to-peer communications while maintaining centralized control of key distribution and management functions.

Finally, it is also an objective of the invention to provide a virtual private network which provides encryption and authentication services for peer-to-peer communications and in which registration is carried out by a central gateway server.

These objectives of the invention are accomplished by providing a virtual private network for communicating between a server and clients over an open network and in which the clients are equipped with an applications level encryption and mutual authentication program which includes at least one shim positioned above either the socket, transport driver interface, or network interface layers of a client computers communications hierarchy, and which intercepts function calls or data packets in order to authenticate the parties to the communication by

Petitioner Apple Inc. - Exhibit 1002, p. 919

establishing secured channels between the server and the parties to the communication, prior to establishment of the secured communications link between the parties, in order to carry out mutual authentication and session key generation functions.

More particularly, according to the principles of a preferred embodiment of the invention, client communications software is provided which, at the socket or transport driver interface levels, intercepts function calls to the socket or transport driver and directs calls to the authentication server in order to perform encryption and authentication routines, and at the network driver interface, performs encryption and authentication functions by intercepting the datagrams or data portions of the packets transmitted by the transport driver interface based on communications between the authentication server and the client. According to this aspect of the invention, a system of providing authentication and encryption services for the purpose of establishing a virtual private network includes a plurality of shims arranged to operate at different protocol levels in order to establish a common secure communications link to an authentication server.

In one especially preferred embodiment of the invention, the client software includes a Winsock shim arranged to intercept function calls to the Winsock library on a client machine and redirect initial communications

Petitioner Apple Inc. - Exhibit 1002, p. 920

through the authentication client software to the authentication server, so that any function calls to the Winsock library of programs are intercepted by the shim and carried out by the applications level security program. In this embodiment, the client authentication software substitutes its own function calls for the original function calls in order to establish a secured communications link to the authentication server over which such functions as mutual authentication between the client and server, indirect authentication of peer applications by the now trusted server, session key generation, are carried out, as well as ancillary functions such as on-line registration (OLR), utilizing the unmodified original Winsock library and TCP/IP communications stacks.

By inserting a shim at the Winsock level, an applications level client/server based security program such as SmartGATE™ can be used to provide secure communications for any application which utilizes the Winsock library. In addition, by including analogous shims at other levels, the invention can be used to secure virtually any communications application, including those which by-pass the TDI layer and communicate directly with the network driver level.

Instead of the current array of mutually exclusive alternative methods and systems of establishing secured communications over an open network, the invention thus

Petitioner Apple Inc. - Exhibit 1002, p. 921

provides a single integrated method and system capable of carrying out both client/server communications and peer-to-peer communications between a wide variety of communications applications regardless of whether the applications use a socket or even commonly accepted internet protocols, with complete mutual authentication and encryption of data files at all levels and between all parties to the network.

It will be appreciated that the term "virtual private network" is not to be taken as limiting, and that the principles of the invention can be applied to any remote access schemes which utilize the Internet or other relatively insecure networks to provide access for remote users, corporate intranets, and electronic commerce.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1A is a schematic diagram of a client/server virtual private network.

Fig. 1B is a schematic diagram of an alternative virtual private network based on peer-to-peer communications.

Fig. 2 is a functional block diagram showing the operation of an applications level security program in a conventional communications network hierarchy.

Petitioner Apple Inc. - Exhibit 1002, p. 922

Fig. 3 is a functional block diagram showing the communications network hierarchy of Fig. 1, modified to provide a second layer of service in accordance with the principles of a preferred embodiment of the invention.

Fig. 4 is a functional block diagram showing the communications network hierarchy of Fig. 2, modified to provide a third layer of service in accordance with the principles of the preferred embodiment.

Fig. 5 is a functional block diagram showing the communication network hierarchy of Fig. 3, modified to provide a fourth layer of service in accordance with the principles of the preferred embodiment.

Fig. 6 is a schematic diagram of a virtual private network utilizing the principles of the preferred embodiment of the invention.

Fig. 7 is a flowchart illustrating a method of implementing the system of the preferred embodiment.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Fig. 2 illustrates the operation of a client authentication program which is utilized in the present invention. An example of such a program is the SmartGATE™ program discussed briefly above, although other

Petitioner Apple Inc. - Exhibit 1002, p. 923

applications level security programs, whether or not token based, could be modified in a manner similar to that discussed in the following description. The illustrated hierarchy is the Windows NT architecture, although versions of SmartGATE™ exist for other architectures, and the invention could easily be adapted for use with any version of SmartGATE™, including UNIX and MacIntosh versions, as well as for use with applications level security programs designed for communications architectures other than those supported by SmartGATE™. Conversely, it is intended that the present invention can be used with authentication and encryption schemes other than that used by SmartGATE™ and disclosed in U.S. Patent No. 5,602,918. For purposes of convenience, therefore, the software represented by SmartGATE™ is simply referred to as client authentication software.

In addition, it noted that the client computer architectures illustrated in Figs. 3-6, which are modified versions of the architecture of Fig. 2, is to be used with an overall network layout such as the one illustrated in Fig. 6, which includes an authentication server that may be a SmartGATE™ server, or another server depending on the client authentication software. The invention is not merely the addition of shims to the client software, but involves the manner in which the shims are used in the establishment of the authentications and key generation links to the server.

Petitioner Apple Inc. - Exhibit 1002, p. 924

Turning to Fig. 2, which provides background for the description of the invention illustrated in Figs. 3-6, the client authentication software 20 is situated above the boundary of the transport or TDI layer 21 and is designed to utilize a socket 22, such as Winsock, to carry out communications with the authentication server 23 shown in Fig. 6 by means of a transport protocol such as TCP/IP, UDP, or the like, which in turn supply datagrams or packets to a hardware driver layer 24, such as NDIS 3.0, of a network or modem connection 25.

In operation, the client authentication software 20 intercepts interconnect calls 26 form client authentication software supported applications 27 and, if the calls are directed to the authentication server 23, or to a server 28 situated on a secured network whose access is controlled by the authentication server, establishes a secured communications link to the server by executing appropriate function calls 29 to the socket library, which in turn transmits function calls 30 to the TDI layer, causing the TDI layer to form datagrams or packets 31. Datagrams or packets 31 are then formatted over packaged for transmission by the hardware drivers 24 and sent to the communications network in the form of Ethernet packets or analog signals 32 containing the original datagrams from the TDI layer. Once the secured communications link has been established, client authentication software 20 encrypts all further data communications 34 from

Petitioner Apple Inc. - Exhibit 1002, p. 925

applications 27, which are indicated by dashed lines, before handing them off to the next lower layer in the form of encrypted files 35. The dashed lines are shown in Fig. 2 as extending only to the TDI layer 21, because the datagrams formed by the TDI layer are indistinguishable as to content, but it is to be understood that datagrams or packets 31 carry both the communications used to establish the secure channel, and the encrypted files subsequently sent therethrough.

Finally, in the case of SmartGATE™, the authentication client software utilizes either a smart card or secured file to supply the secret keys used during authentication to generate a session key for encryption of further communications, and also to carry out certain other encryption and authentication functions, although it is of course within the scope of the invention to use key distribution and authentication methods which do not rely on smartcards or tokens, and the tokens are not involved in any of the basic communications functions of the client authentication software 20.

In addition to the applications 27 which communicate with the server via the authentication/encryption software 20, a typical system will have a number of additional software applications 36 and 37 capable of carrying out communications over the open network, but which the authentication client software is not configured to handle,

Petitioner Apple Inc. - Exhibit 1002, p. 926

and which are not specifically adapted or intended to carry out communications with the authentication server. These are referred to herein as peer-to-peer applications, and can include applications which use the same sockets as the authentication client software, applications which directly call upon a transport driver interface stack, whether using the same protocol as the authentication client software or another protocol, all of which are intended to be represented by the TDI layer, and applications which are written to call directly upon the hardware drivers. These peer-to-peer applications may have their own encryption and authentication capabilities, but cannot utilize the services of the authentication server or client software, and therefore the function calls made by the applications and the files transmitted are indicated by separate reference numerals 40-43.

It will be appreciated by those skilled in the art that lower layer application programs which generate packets in forms other than those represented by the TDI layer are also possible, and should be considered within the scope of the invention, but at present virtually all open network applications use at least one of the TDI protocols, and thus while these programs may interact directly with the network driver layer, and require a network driver layer shim, as will be discussed below, are illustrated for purposes of convenience as part of the TDI layer applications.

Petitioner Apple Inc. - Exhibit 1002, p. 927

Turning now to a preferred embodiment of the invention, the arrangement shown in Fig. 3 modifies the arrangement of Fig. 2 by adding a socket shim 50 between the socket 22 utilized by the authentication client software 20, the peer-to-peer applications 36 which also utilize the socket 20, and the authentication client software itself. The shim 50 operates by hooking or intercepting call initiation function calls 40 made to the socket and, in response thereto, having the authentication client software initiate communications with the authentication server 23, shown in Fig. 6, in order to carry out the authentication protocol, as will be discussed in more detail below. Shim 50 also causes files 41 intended for the TDI layer to be diverted to the authentication software for encryption based on the session keys generated during the initial communications with the authentication server, and transmission as encrypted files 51 addressed to the peer application, also shown in Fig. 6, which could also be an application on the application server 28.

Since the basic authentication client software is designed to send all communications directly to the authentication server, while the peer-to-peer applications are designed only to communicate with "peers" 45 and not with the authentication server, the principal function of shim 50 is to arrange for the destination of address of the communication to be supplied to both the authentication

Petitioner Apple Inc. - Exhibit 1002, p. 928

client software and to authentication server, even though the peer application assumes that it is communicating only with the peer application. This function permits session key encrypted communications to be forwarded directly to the peer application, as illustrated in Fig. 6, while the latter function provides the authentication server with the client address so that the authentication server can establish a secured and authenticated link with the peer application, via authentication client software on the peer computer, and transmit the session key to the peer application or at least enable the peer application to recreate the session so that it can decrypt the encrypted files received directly from the client application.

Thus, while it is appreciated that the use of socket shims is well-known, as mentioned above, the socket shim shown in Fig. 2 has the unique function of enabling direct peer-to-peer communications with mediation by the authentication server, permitting the highest level of authentication service and collateral functions. In addition, because of the mediation by the key server, the peer applications do not need to have a shared secret key, allowing centralized key management, with only the authentication server having access to all of the client's secret keys.

Figs. 4 shows the variation of the client authentication software 20 in which a TDI shim 52 similar

Petitioner Apple Inc. - Exhibit 1002, p. 929

in function to the socket shim 50 is provided above the TDI layer. Like the socket shim, implementation of the TDI shim essentially simply involves diverting certain information to the client software in order to establish a communications link with the authentication server, and subsequently perform encryption to obtain encrypted files 54 for transmission directly through the TDI layer in the usual manner. As with the socket shim, TDI shims are not new and can be implemented in known manner, by intercepting TDI service requests, but with the difference from prior TDI shims that the TDI shim works with the authentication software 20 and authentication server to authenticate communications and generate a session key.

Finally, as shown in Fig. 5, a further layer of authentication and encryption may be added by adding a network driver shim 55, either to the arrangement shown in Fig. 3 without the TDI shim, in combination with the TDI shim shown in Fig. 4, or in combination with the TDI shim of Fig. 4 but not the socket shim, to provide for authentication of communications at the network driver layer. At this layer, the shim 55 intercepts IP packets from applications 56, but instead of referring back to the applications level routine, checks the destination address (which can be in TCP format, UDP format, and so forth), establishes a session key by communications with the authentication server, converts the session key into a format which can be used to encrypt the IP packet, and

Petitioner Apple Inc. - Exhibit 1002, p. 930

sends the IP packet towards the destination, all by carrying out the necessary operations at the network driver level, in a manner similar to that utilized by the above-mentioned SnareNet software program, but with the difference that the authenticating communications link and key generation is carried out by packets addressed to a corresponding layer 56 of the authentication server, which may be further connected to an applications server 57.

It will be noted that since the IP packets are not distinguishable by content, the network driver layer shim could be used as an additional level of security, rather than as an alternative to applications level encryption, with the encrypted files generated by software 20 being further encrypted by shim 55 before transmission to the authentication server or associated gateway.

The overall system utilizing the authentication client software illustrated in Figs. 3-5 is schematically illustrated in Fig. 6. The principal components of the overall system are the client computers containing software of the type illustrated in Figs. 2-5, including client authentication software 20 and shims 50, 53, and/or 55, and applications with communications capabilities (represented by applications 27, 36, 37, and 56 on one client, and application 45 on the other). For purposes of illustration, the client of Figs. 6 is thus depicted as including applications for communicating at the highest

Petitioner Apple Inc. - Exhibit 1002, p. 931

levels, such as the SmartGATE™ proxy application, applications for communicating at the network driver level with corresponding applications connected to the lower layer of the authentication server, and peer-to-peer applications with no capability of communicating with SmartGATE™, but which use sockets or TDI protocols recognized by the shims.

In the case of the SmartGATE™ proxy application, communications are established in the same manner as in the currently available version of the SmartGATE™ authentication client software, and as described in U.S. Patent No. 5,602,918, the communications link being indicated by arrows 60 and 61, with arrow 60 representing the client/server response channel used to authenticate the parties and generate the session key.

In the case of a peer-to-peer application, in which the clients wish to communicate over a direct link 62, the invention provides for the function calls establishing the communications to be intercepted and the initialization procedure routed through channel 61 to the authentication server 23. Server 23 then opens a secured channel 63 to the authentication client software 20 associated with peer application 45 by performing the same mutual authentication procedure performed for the purpose of establishing channel 63, and once the channel is established with its own session key, transmits information using the channel 63

Petitioner Apple Inc. - Exhibit 1002, p. 932

session key which allows the client to recreate the channel 60 session key for use in decrypting communications sent over channel 62. Alternatively, after establishing channel 63, the channel 60 session key could be used to transmit back to the original sending party information necessary to recreate the channel 63 session key. In either case, the authentication server is thus used to establish a fully authenticated "tunnel" between the peer applications without the need to modify any of the sockets, TDI protocols, or hardware drivers on either of the client computers. While the transmitting peer application has no way of directly authenticating the receiving peer, only a receiving peer authenticated by the authentication server will be able to generate the necessary session keys, and thus each of the parties to the communication is effectively authenticated.

For the lower layer application 56, a similar protocol may be employed, in which the attempted communication between lower layer applications is intercepted, and the communications link to the authentication server is used to generate a session key, which is then used to encrypt the packets or datagrams being sent. In this case, the destination must be the lower layer of the authentication server, and thus the communications link is indicated by a separate channel 67.

Petitioner Apple Inc. - Exhibit 1002, p. 933

Finally, the procedures associated with the network illustrated in Fig. 6 are summarized in the flowchart of Fig. 7. For communications directly with the applications level portion of the server 23, steps 100-103 are used, while for peer-to-peer communications, steps 104-109 are used, and for network driver level communications, steps 110-114 are used.

In particular, step 100 by which the applications level authentication program 20 illustrated in Figs. 3-5 receives a call initiation request, either directly from a supported applications program 27 or from a programs 36 and 37 via one of the shims 50 and 53, step 101 is step by which the program 20 addresses the authentication server, step 102 is the step by which the client and server are mutually authenticated and the session keys generated using, for example, the procedure described in U.S. Patent No. 5,602,918, and step 103 is the step by which program 20 encrypts further communications received directly or via shims 50 and 53 from the applications programs 27, 36, and 37.

For peer-to-peer communications, step 105, which is part of step 100, is the step by which the peer address is supplied to program 20, steps 106 and 107 are identical to steps 101 and 102, step 108 is the step by which communications channel 63 shown in Figure 6 is established, step 109 is the step by which the destination computer

Petitioner Apple Inc. - Exhibit 1002, p. 934

authenticated by the server is enabled to decrypt communications received over channel 62, and step 110 is the step by which program 20 encrypts the communications. It will of course be appreciated that these steps represent only a summary of the steps involved in carrying out the present invention, and that further steps will be apparent to those skilled in the art based on the above description of the apparatus and software portions of the preferred embodiment of the invention.

Having thus described various preferred embodiments of the invention, those skilled in the art will appreciate that variations and modifications of the preferred embodiment may be made without departing from the scope of the invention. It is accordingly intended that the invention not be limited by the above description or accompanying drawings, but that it be defined solely in accordance with the appended claims.

Petitioner Apple Inc. - Exhibit 1002, p. 935

I claim:

1. Apparatus for carrying out communications over a multi-tier virtual private network, said network including a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network, comprising:

means for intercepting function calls and requests for service sent by an applications program on one of said client computers to a lower level set of communications drivers; and

means for causing an applications level authentication and encryption program in said one of said client computers to communicate with the server, generate said session key, and encrypt files sent by the applications program before transmittal over said open network.

2. Apparatus as claimed in claim 1, further comprising means for intercepting files packaged by a transport driver interface layer to form packets and encrypting the packets using a session key generated during communications with a lower layer of the server.

3. A method as claimed in claim 1, further comprising

means for intercepting a destination address during initialization of communications between said one of said

Petitioner Apple Inc. - Exhibit 1002, p. 936

client computers and a second of said client computers on said virtual private network;

means for causing said applications level authentication and encryption program to communicate with the server to carry out functions a.) and b.);

means for transmitting said destination address to said server;

means for causing said server to carry-out functions a.) and b.) with respect to the second of said two client computers;

means for enabling said second of said two client computers to recreate the session key;

means for causing said authentication software to encrypt files to be sent to the destination address using the session key; and

means for transmitting the encrypted files directly to the destination address.

4. Apparatus as claimed in claim 3, wherein said means for intercepting the destination address is carried out by a shim positioned between a peer-to-peer applications program and a layer of a communications driver architecture of said one of the two client computers.

5. A multi-tier virtual private network, comprising:

a server and a plurality of client computers, the server and client computers each including means for

Petitioner Apple Inc. - Exhibit 1002, p. 937

transmitting data to and receiving data from an open network,

wherein said means for transmitting data to and receiving data from the open network includes, in any client computer initiating communications with the server:

applications level encryption and authentication software arranged to communicate with the server in order to: a.) mutually authenticate the server and the client computer initiating communications with the server and b.) generate a session key for use by the client computer initiating communications to encrypt files;

at least one lower level set of communications drivers;

and a shim arranged to intercept function calls and requests for service sent by an applications program to the lower level set of communications drivers in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files sent by the applications program before transmittal over said open network.

6. A multi-tier virtual private network as claimed in claim 5, wherein said lower level set of communications drivers includes a network driver layer, a transport driver

Petitioner Apple Inc. - Exhibit 1002, p. 938

interface layer arranged to package applications files as packets capable of being routed over the open network and supply the packets to the network driver layer for transmission to the open network, and an applications socket for facilitating service requests by said applications program to the transport driver interface layer, and wherein said shim is a socket shim positioned between the applications program and the socket to intercept function calls to the socket in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files sent by the applications program before the files are packaged by the transport driver interface layer.

7. A multi-tier virtual private network as claimed in claim 6, wherein said applications program is a peer-to-peer communications program, and wherein a peer application destination address, included in said function calls to the socket, is diverted by the socket shim and wherein a destination address including said intercepted function calls is supplied to the server during communications with the server, causing the service to establish a communications link with a peer application, mutually authenticate the peer application, and enable the peer application to reconstruct the session key in order to receive encrypted files sent by the peer-to-peer communications program over the open network.

Petitioner Apple Inc. - Exhibit 1002, p. 939

8. A multi-tier virtual private network as claimed in claim 6, further including a transport driver interface shim positioned between the transport driver interface layer and a second applications program, for intercepting requests from the second applications program for service by the transport driver interface layer in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files sent by the applications program before the files are packaged by the transport driver interface layer.

9. A multi-tier virtual private network as claimed in claim 8, further comprising a network driver layer shim positioned between the network driver layer and the transport driver interface layer and arranged to intercept files packaged by the transport driver interface layer and encrypt the files using a session key generated during communications with a lower layer of the server.

10. A multi-tier virtual private network as claimed in claim 5, wherein said lower level set of communications drivers includes a network driver layer, and a transport driver interface layer arranged to package applications files as packets capable of being routed over the open network and supply the packets to the network driver layer for transmission to the open network, and wherein said shim is a transport driver interface layer shim positioned

Petitioner Apple Inc. - Exhibit 1002, p. 940

between the applications program and the transport driver interface layer to intercept service requests by the applications program to the transport driver interface layer in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files sent by the applications program before the files are packaged by the transport driver interface layer.

11. A multi-tier virtual private network as claimed in claim 10, wherein said applications program is a peer-to-peer communications program, and wherein a peer application destination address, included in said intercepted requests for service, is diverted by the transport driver interface layer shim and supplied to the server during communications with the server, causing the service to establish a communications link with a peer application, mutually authenticate the peer application, and enable the peer application to reconstruct the session key in order to receive encrypted files sent by the peer-to-peer communications program over the open network.

12. A multi-tier virtual private network as claimed in claim 10, further comprising a network driver layer shim positioned between the network driver layer and the transport driver interface layer and arranged to intercept files packaged by the transport driver interface layer and

Petitioner Apple Inc. - Exhibit 1002, p. 941

encrypt the files using a session key generated during communications with a lower layer of the server.

13. A multi-tier virtual private network, comprising:

a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network,

wherein said means for transmitting data to and receiving data from the open network includes, in any client computer initiating communications with the server:

applications level encryption and authentication software arranged to communicate with the server in order to: a.) mutually authenticate the server and the client computer initiating communications with the server and b.) generate a session key for use by the client computer initiating communications to encrypt files; and

at least one lower level set of communications drivers,

wherein said lower level set of communications drivers includes a network driver layer, a transport driver interface layer arranged to package applications files as packets capable of being routed over the open network and supply the packets to the network driver layer for transmission to the open network, and a

Petitioner Apple Inc. - Exhibit 1002, p. 942

network driver layer shim positioned between the transport driver interface layer and the network driver layer and arranged to intercept files packaged by the transport driver interface layer and encrypt the files using a session key generated during communications with a lower layer of the server.

14. A multi-tier virtual private network, comprising:

a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network,

wherein said means for transmitting data to and receiving data from the open network includes, in any client computer initiating communications with the server:

applications level encryption and authentication software arranged to communicate with the server in order to: a.) mutually authenticate the server and the client computer initiating communications with the server and b.) generate a session key for use by the client computer initiating communications to encrypt files; and

further comprising means for securing peer-to-peer communications between applications on two of said client computers, said peer-to-peer communications securing means comprising:

Petitioner Apple Inc. - Exhibit 1002, p. 943

means for intercepting a destination address during initialization of communications by a first of said two client computers;

means for causing said authentication software to communicate with the server to carry out functions a.) and b.);

means for transmitting said destination address to said server;

means for causing said server to carry-out functions a.) and b.) with respect to the second of said two client computers;

means for enabling said second of said two client computers to recreate the session key;

means for causing said authentication software to encrypt files to be sent to the destination address using the session key;

means for transmitting the encrypted files directly to the destination address.

15. A multi-tier virtual private network as claimed in claim 14, wherein said means for intercepting the destination address comprises a shim positioned between the peer-to-peer applications program and a layer of a communications driver architecture of said first of the two client computers.

16. A multi-tier virtual private network as claimed in claim 5, wherein said shim is positioned above a socket,

Petitioner Apple Inc. - Exhibit 1002, p. 944

the socket being positioned above a transport driver layer of said communications driver architecture.

17. A multi-tier virtual private network as claimed in claim 5, wherein said shim is positioned above a transport driver layer of said communications driver architecture.

18. Computer software for installation on a client computer of a multi-tier virtual private network, said network including a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network,

wherein said computer software includes:

applications level encryption and authentication software arranged to communicate with the server in order to: a.) mutually authenticate the server and the client computer initiating communications with the server and b.) generate a session key for use by the client computer initiating communications to encrypt files;

and a shim arranged to intercept function calls and requests for service sent by an applications program to a lower level set of communications drivers in order to cause the applications level authentication and encryption program to communicate with the server, generate

Petitioner Apple Inc. - Exhibit 1002, p. 945

said session key, and encrypt files sent by the applications program before transmittal over said open network.

19. Computer software as claimed in claim 18, wherein said lower level set of communications drivers includes a network driver layer, a transport driver interface layer arranged to package applications files as packets capable of being routed over the open network and supply the packets to the network driver layer for transmission to the open network, and an applications socket for facilitating service requests by said applications program to the transport driver interface layer, and wherein said shim is a socket shim positioned between the applications program and the socket to intercept function calls to the socket in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files sent by the applications program before the files are packaged by the transport driver interface layer.

20. Computer software as claimed in claim 19, wherein said applications program is a peer-to-peer communications program, and wherein a peer application destination address, included in said function calls to the socket, is diverted by the socket shim and wherein a destination address including said intercepted function calls is supplied to the server during communications with the

Petitioner Apple Inc. - Exhibit 1002, p. 946

server, causing the service to establish a communications link with a peer application, mutually authenticate the peer application, and enable the peer application to reconstruct the session key in order to receive encrypted files sent by the peer-to-peer communications program over the open network.

21. Computer software as claimed in claim 19, further including a transport driver interface shim positioned between the transport driver interface layer and a second applications program, for intercepting requests from the second applications program for service by the transport driver interface layer in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files sent by the applications program before the files are packaged by the transport driver interface layer.

22. Computer software as claimed in claim 21, further comprising a network driver layer shim positioned between the network driver layer and the transport driver interface layer and arranged to intercept files packaged by the transport driver interface layer and encrypt the files using a session key generated during communications with a lower layer of the server.

23. Computer software as claimed in claim 18, wherein said lower level set of communications drivers includes a

Petitioner Apple Inc. - Exhibit 1002, p. 947

network driver layer, and a transport driver interface layer arranged to package applications files as packets capable of being routed over the open network and supply the packets to the network driver layer for transmission to the open network, and wherein said shim is a transport driver interface layer shim positioned between the applications program and the transport driver interface layer to intercept service requests by the applications program to the transport driver interface layer in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files sent by the applications program before the files are packaged by the transport driver interface layer.

24. Computer software as claimed in claim 23, wherein said applications program is a peer-to-peer communications program, and wherein a peer application destination address, included in said intercepted requests for service, is diverted by the transport driver interface layer shim and supplied to the server during communications with the server, causing the service to establish a communications link with a peer application, mutually authenticate the peer application, and enable the peer application to reconstruct the session key in order to receive encrypted files sent by the peer-to-peer communications program over the open network.

Petitioner Apple Inc. - Exhibit 1002, p. 948

25. Computer software as claimed in claim 23, further comprising a network driver layer shim positioned between the network driver layer and the transport driver interface layer and arranged to intercept files packaged by the transport driver interface layer and encrypt the files using a session key generated during communications with a lower layer of the server.

26. Computer software for installation on a client computer of a multi-tier virtual private network, said network including a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network,

wherein said computer software includes:

applications level encryption and authentication software arranged to communicate with the server in order to: a.) mutually authenticate the server and the client computer initiating communications with the server and b.) generate a session key for use by the client computer initiating communications to encrypt files; and

at least one lower level set of communications drivers,

wherein said lower level set of communications drivers includes a network driver layer, a transport driver interface layer

Petitioner Apple Inc. - Exhibit 1002, p. 949

arranged to package applications files as packets capable of being routed over the open network and supply the packets to the network driver layer for transmission to the open network, and a network driver layer shim positioned between the transport driver interface layer and the network driver layer and arranged to intercept files packaged by the transport driver interface layer and encrypt the files using a session key generated during communications with a lower layer of the server.

27. Computer software for installation on a client computer of a multi-tier virtual private network, said network including a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network,

wherein said computer software includes:

applications level encryption and authentication software arranged to communicate with the server in order to: a.) mutually authenticate the server and the client computer initiating communications with the server and b.) generate a session key for use by the client computer initiating communications to encrypt files; and

further comprising means for securing peer-to-peer communications between applications on two of said client

Petitioner Apple Inc. - Exhibit 1002, p. 950

computers, said peer-to-peer communications securing means comprising:

means for intercepting a destination address during initialization of communications by a first of said two client computers;

means for causing said authentication software to communicate with the server to carry out functions a.) and b.);

means for transmitting said destination address to said server;

means for causing said server to carry-out functions a.) and b.) with respect to the second of said two client computers;

means for enabling said second of said two client computers to recreate the session key;

means for causing said authentication software to encrypt files to be sent to the destination address using the session key;

means for transmitting the encrypted files directly to the destination address.

28. Computer software as claimed in claim 27, wherein said means for intercepting the destination address comprises a shim positioned between the peer-to-peer applications program and a layer of a communications driver architecture of said first of the two client computers.

Petitioner Apple Inc. - Exhibit 1002, p. 951

29. Computer software as claimed in claim 27, wherein said shim is positioned above a socket, the socket being positioned above a transport driver layer of said communications driver architecture.

30. Computer software as claimed in claim 27, wherein said shim is positioned above a transport driver layer of said communications driver architecture.

31. A method of carrying out communications over a multi-tier virtual private network, said network including a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network, comprising the steps of:

intercepting function calls and requests for service sent by an applications program in one of said client computers to a lower level set of communications drivers;

causing an applications level authentication and encryption program said one of said client computers to communicate with the server, generate said session key, and encrypt files sent by the applications program before transmittal over said open network.

32. A method as claimed in claim 31, further comprising the step of intercepting files packaged by a transport driver interface layer to form packets and encrypting the

Petitioner Apple Inc. - Exhibit 1002, p. 952

packets using a session key generated during communications with a lower layer of the server.

33. A method as claimed in claim 31, further comprising the step of intercepting a destination address during initialization of communications between said one of said client computers and a second of said client computers on said virtual private network;

causing said applications level authentication and encryption program to communicate with the server to carry out functions a.) and b.);

transmitting said destination address to said server;

causing said server to carry-out functions a.) and b.) with respect to the second of said two client computers;

enabling said second of said two client computers to recreate the session key;

causing said authentication software to encrypt files to be sent to the destination address using the session key; and

transmitting the encrypted files directly to the destination address.

34. A method as claimed in claim 33, wherein said step of intercepting the destination address is carried out by a shim positioned between a peer-to-peer applications program

Petitioner Apple Inc. - Exhibit 1002, p. 953

and a layer of a communications driver architecture of said one of the two client computers.

Petitioner Apple Inc. - Exhibit 1002, p. 954

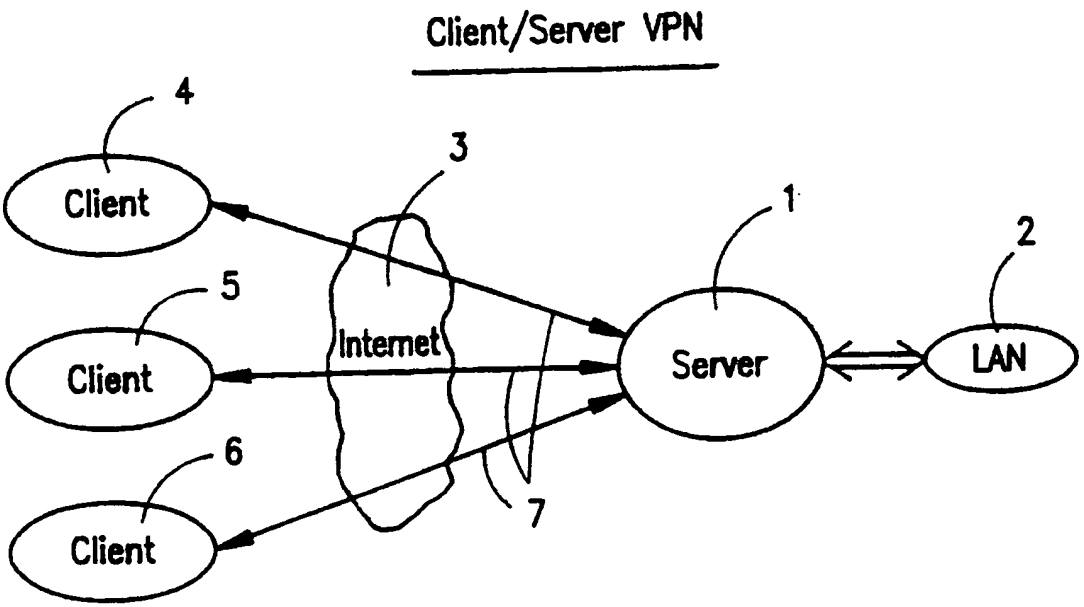


FIG. 1A
(PRIOR ART)

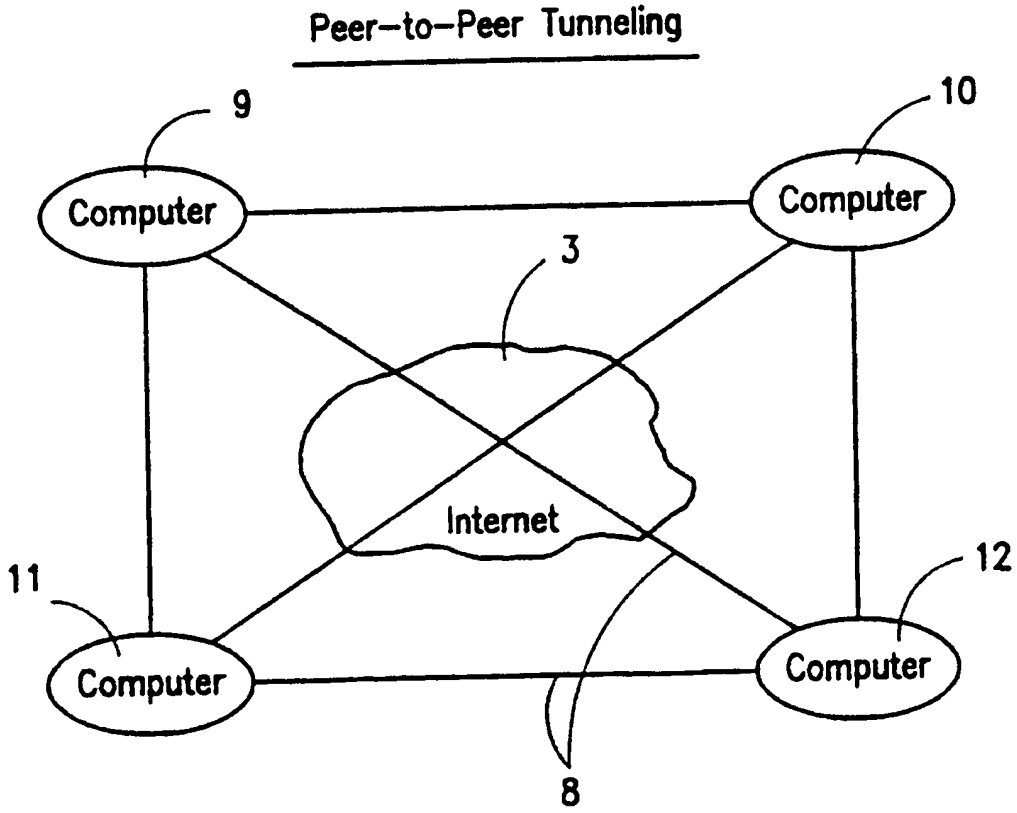


FIG. 1B

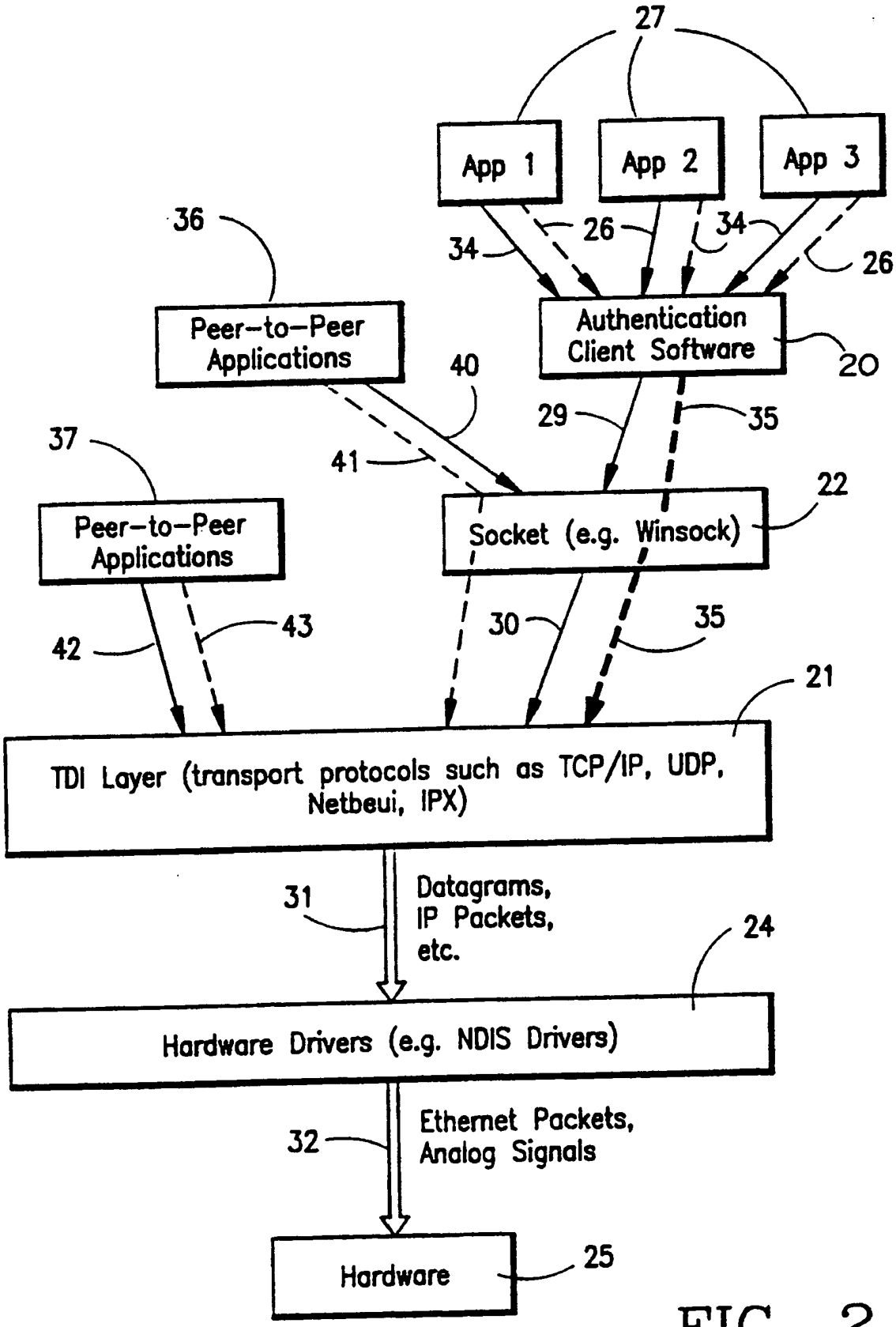


FIG. 2
(PRIOR ART)

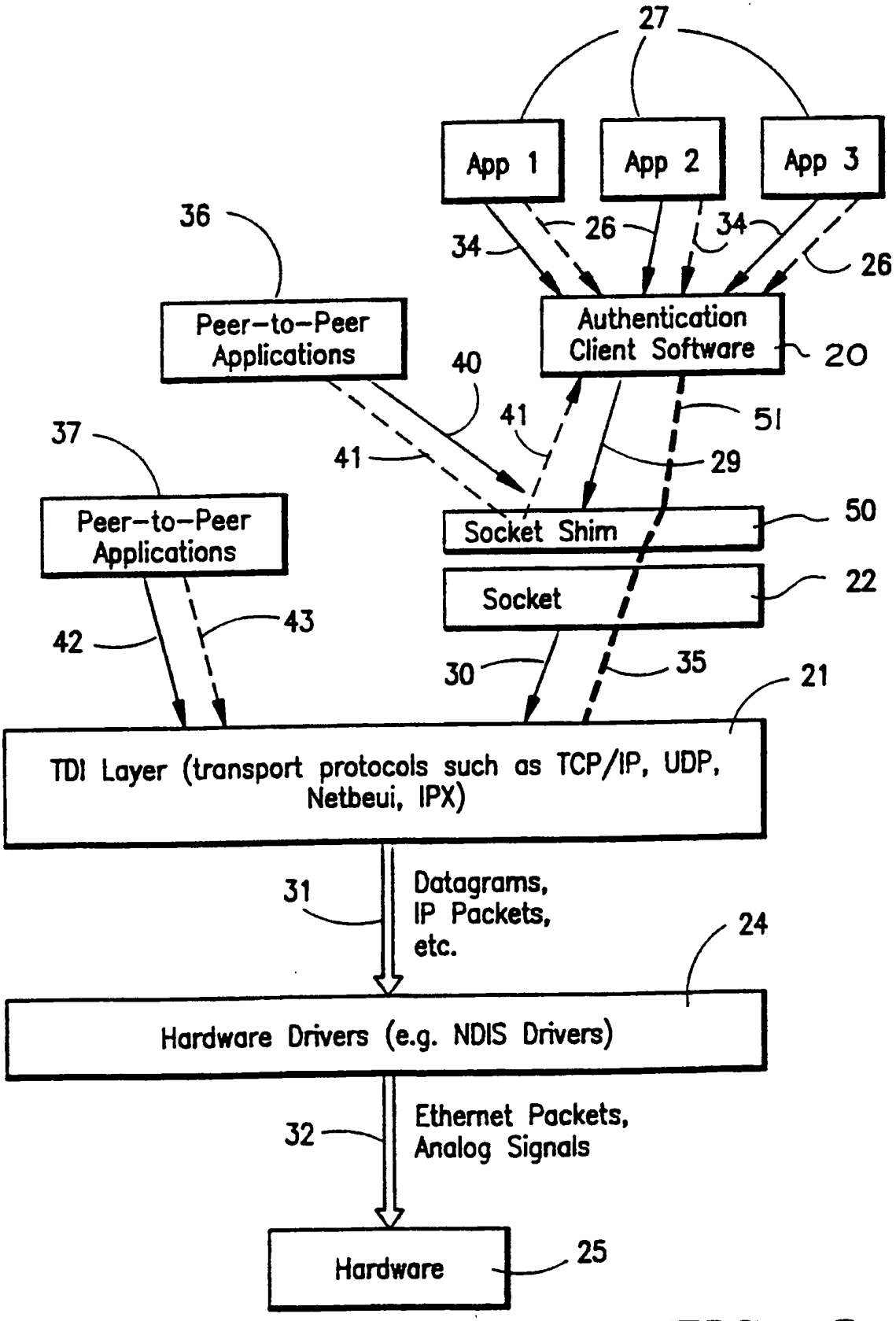

27
App 1
App 2
App 3
36
34
26
34
26
Peer-to-Peer Applications
Authentication Client Software
20
40
41
51
37
41
29
Peer-to-Peer Applications
Socket Shim
50
Socket
22
42
43
30
35
21
TDI Layer (transport protocols such as TCP/IP, UDP, Netbeui, IPX)
31
Datagrams, IP Packets, etc.
24
Hardware Drivers (e.g. NDIS Drivers)
32
Ethernet Packets, Analog Signals
Hardware
25

FIG. 3

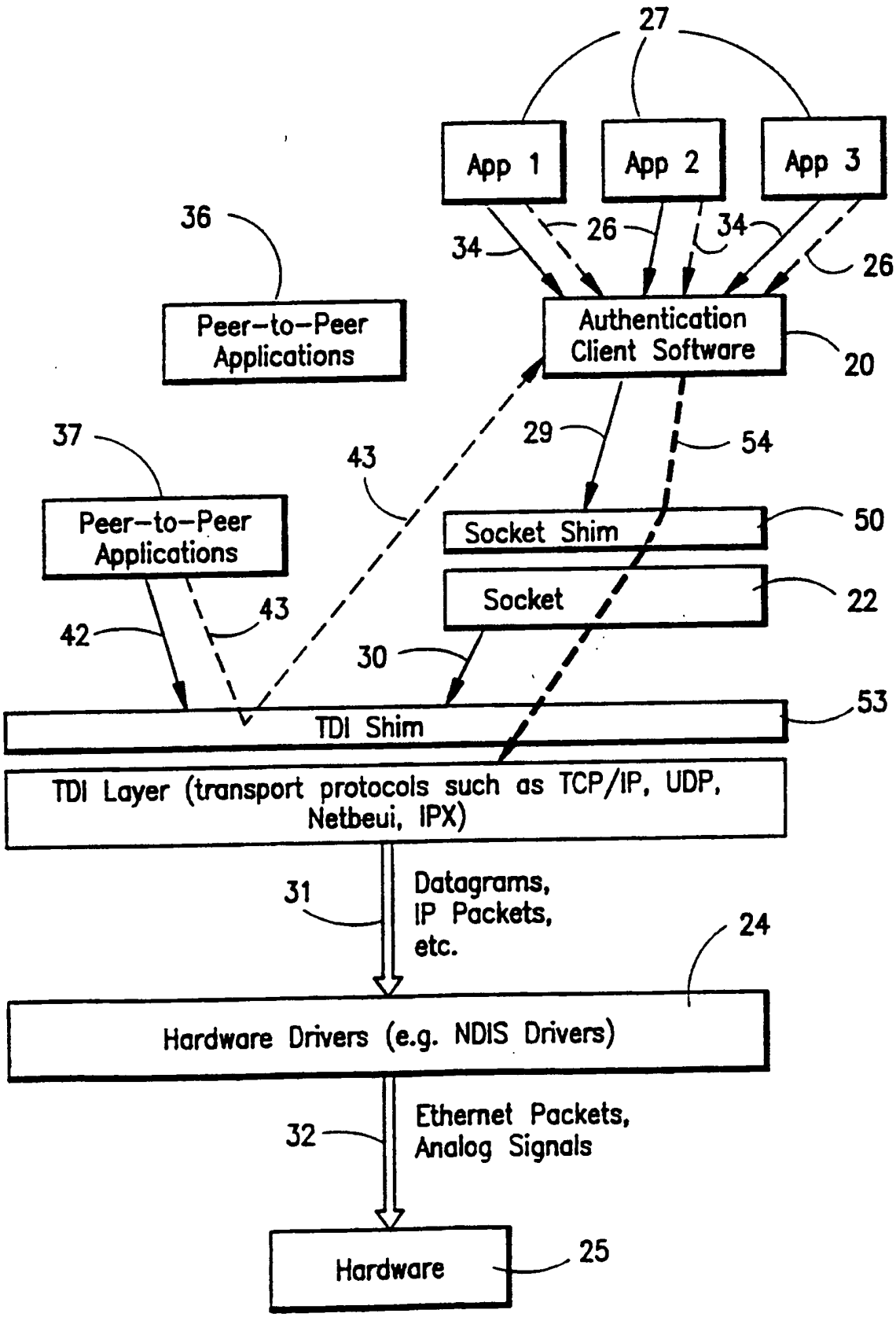

27
App 1
App 2
App 3
36
34
26
34
26
Peer-to-Peer Applications
Authentication Client Software
20
37
29
54
43
Peer-to-Peer Applications
Socket Shim
50
Socket
22
43
42
30
TDI Shim
53
TDI Layer (transport protocols such as TCP/IP, UDP, Netbeui, IPX)
31
Datagrams, IP Packets, etc.
24
Hardware Drivers (e.g. NDIS Drivers)
32
Ethernet Packets, Analog Signals
Hardware
25

FIG. 4

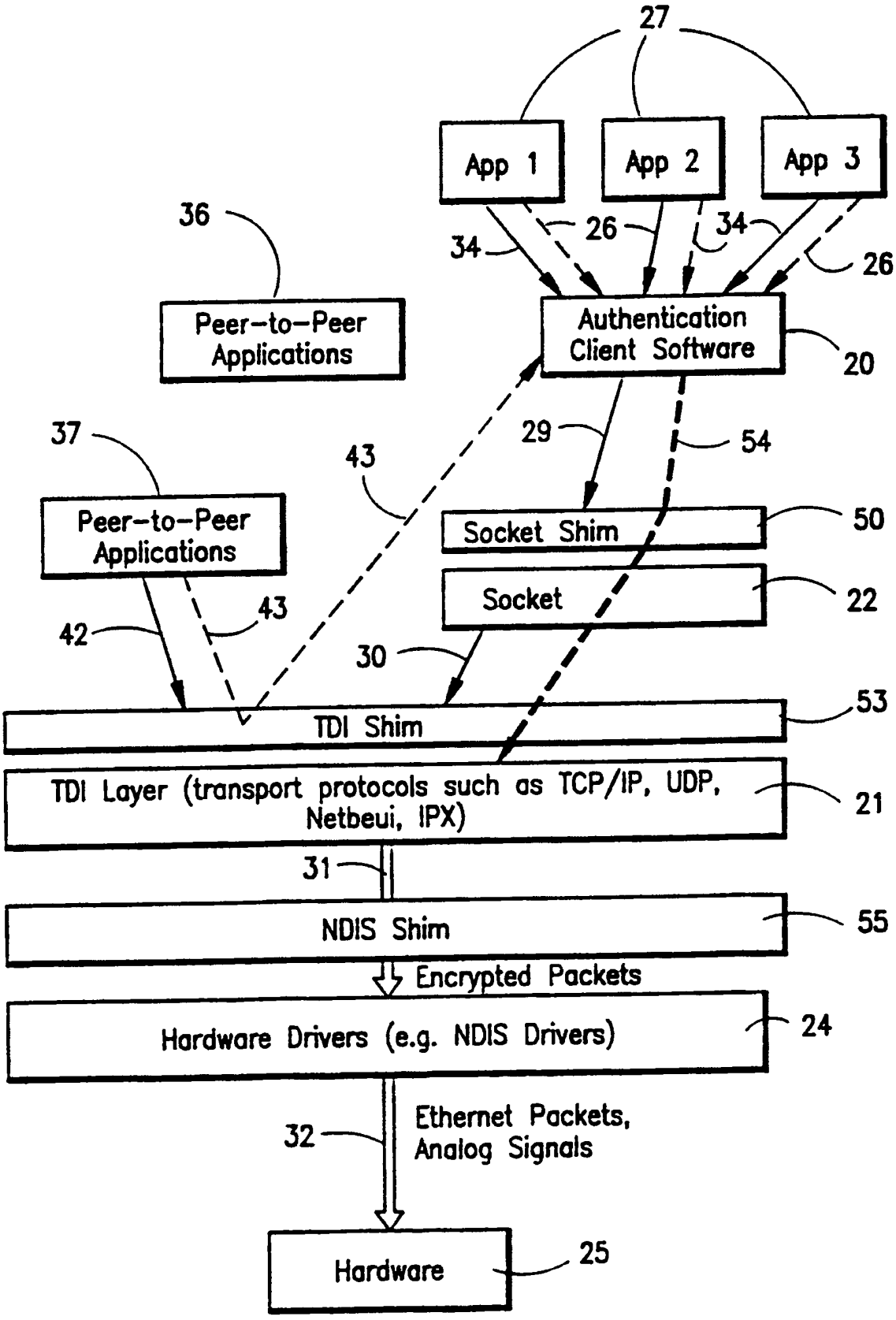

27
App 1
App 2
App 3
36
34
26
34
26
Peer-to-Peer Applications
Authentication Client Software
20
37
29
54
43
Peer-to-Peer Applications
Socket Shim
50
Socket
22
43
42
30
TDI Shim
53
TDI Layer (transport protocols such as TCP/IP, UDP, Netbeui, IPX)
21
31
NDIS Shim
55
Encrypted Packets
Hardware Drivers (e.g. NDIS Drivers)
24
32
Ethernet Packets, Analog Signals
Hardware
25

FIG. 5

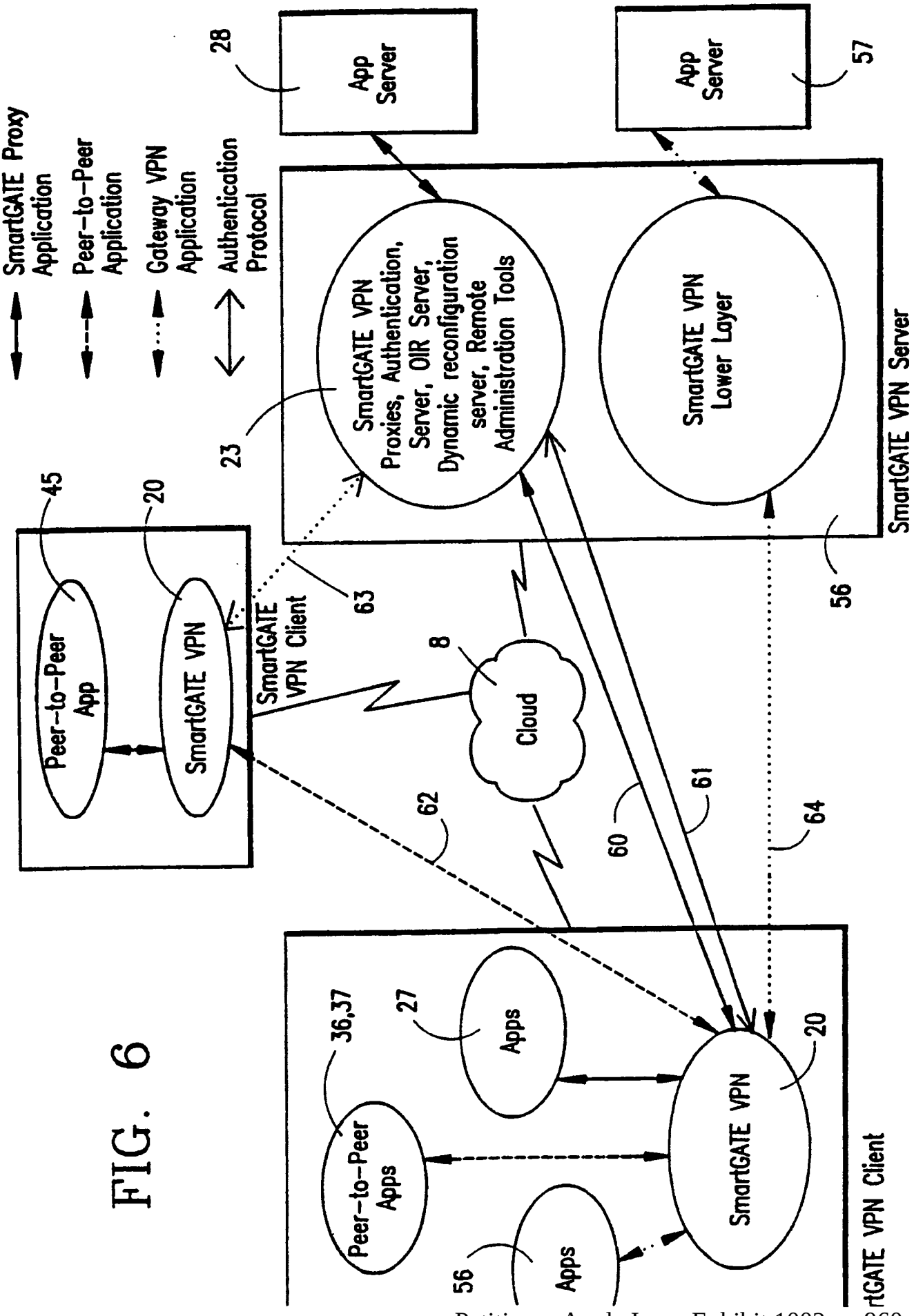

SmartGATE Proxy Application
Peer-to-Peer Application
Gateway VPN Application
Authentication Protocol
28
App Server
57
App Server
23
SmartGATE VPN Proxies, Authentication, Server, OIR Server, Dynamic reconfiguration server, Remote Administration Tools
SmartGATE VPN Lower Layer
SmartGATE VPN Server
56
45
20
Peer-to-Peer App
SmartGATE VPN
SmartGATE VPN Client
63
8
Cloud
62
60
61
64
36,37
27
Apps
Peer-to-Peer Apps
SmartGATE VPN
20
56
Apps
rtGATE VPN Client

FIG. 6

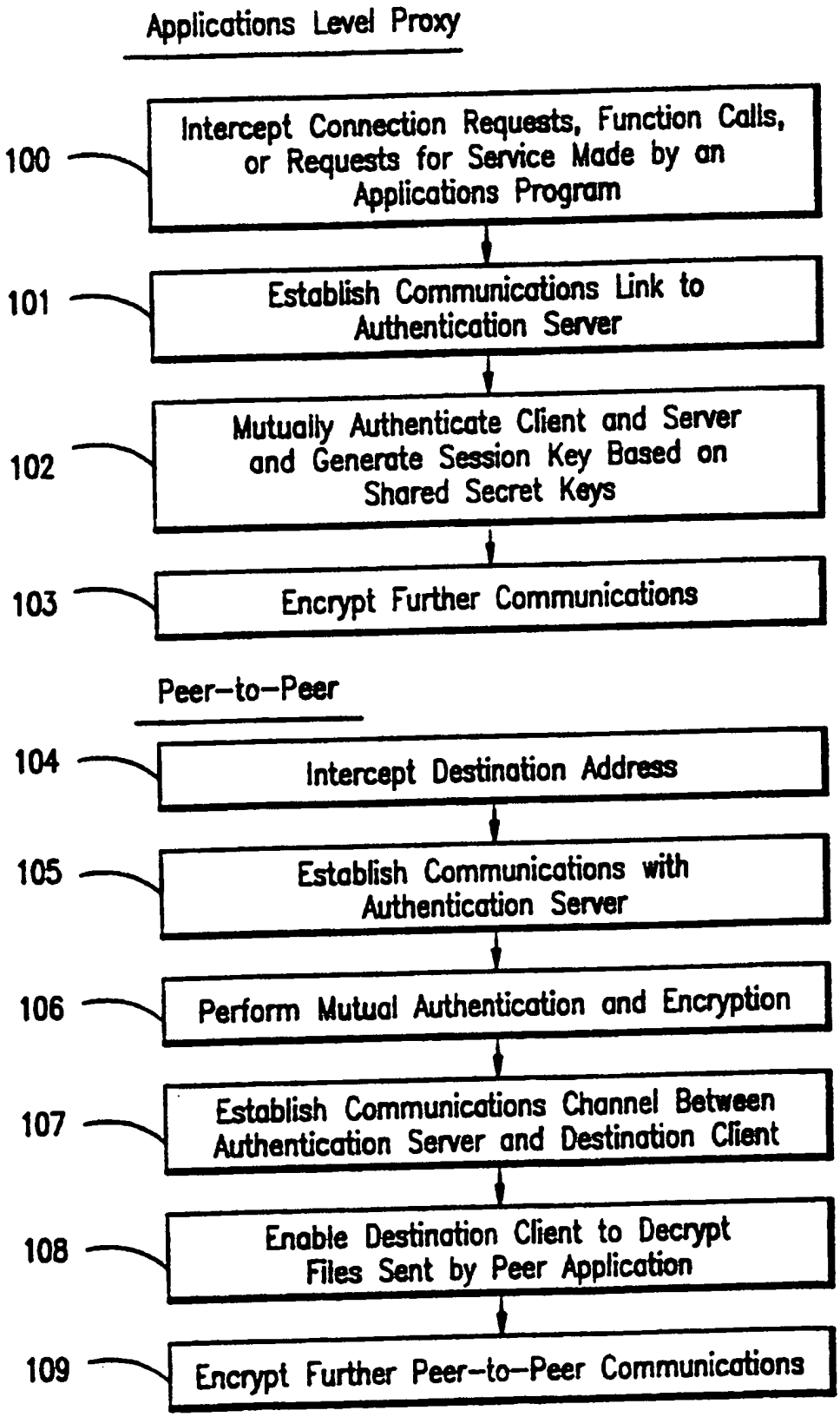

Applications Level Proxy
100
Intercept Connection Requests, Function Calls, or Requests for Service Made by an Applications Program
101
Establish Communications Link to Authentication Server
102
Mutually Authenticate Client and Server and Generate Session Key Based on Shared Secret Keys
103
Encrypt Further Communications
Peer-to-Peer
104
Intercept Destination Address
105
Establish Communications with Authentication Server
106
Perform Mutual Authentication and Encryption
107
Establish Communications Channel Between Authentication Server and Destination Client
108
Enable Destination Client to Decrypt Files Sent by Peer Application
109
Encrypt Further Peer-to-Peer Communications

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/17198

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/00
US CL :395/187.01

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 395/187.01, 186, 188.01, 200.17, 200.12; 380/49, 21, 25, 4

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS, STN, IEEE ProQuest
search terms: virtual private network, shims, DLLs, protocol layers, Winsock, sockets, encryption, authentication.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,657,390 A (ELGAMAL ET AL) 12 AUGUST 1997, FIGURES 1-8, COL. 3, LINES 20-55, COL. 5, LINE 15 TO COL. 8, LINE 32, COL. 11, LINE 1 TO COL. 16, LINE 49.	1,5,6,16,17,18,19,23,31
A	US 5,602,918 A (CHEN ET AL) 11 FEBRUARY 1997, SEE ENTIRE PATENT.	1-34
A	US 5,550,984 A (GELB) 27 AUGUST 1996, ABSTRACT, COL. 3, LINE 52 TO COL. 4, LINE 45, COL.6, LINES 27-55.	1-34
Y	HURWICZ, A VIRTUAL PRIVATE AFFAIR, BYTE MAGAZINE, JULY 1997, PAGES 79-87.	1,5,6,16,17,18,19,23,31

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	
"A" document defining the general state of the art which is not considered to be of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"E" earlier document published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 22 OCTOBER 1998	Date of mailing of the international search report 12 NOV 1998
Name and mailing address of the ISA/US	Authorized officer

C24

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 August 2001 (23.08.2001)

PCT

(10) International Publication Number
WO 01/61922 A2

(51) International Patent Classification[7]: H04L 12/00

(21) International Application Number: PCT/US01/04340

(22) International Filing Date: 12 February 2001 (12.02.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/504,783 15 February 2000 (15.02.2000) US

(63) Related by continuation (CON) or continuation-in-part (CIP) to earlier application:
US 09/504,783 (CON)
Filed on 15 February 2000 (15.02.2000)

(71) Applicant *(for all designated States except US)*: **SCIENCE APPLICATIONS INTERNATIONAL CORPORATION** [US/US]; 10260 Campus Point Drive, San Diego, CA 92121 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MUNGER, Edmund, Colby** [US/US]; 1101 Opaca Court, Crownsville, MD 21032 (US). **SCHMIDT, Douglas, Charles** [US/US]; 230 Oak Court, Severna Park, MD 21146 (US). **SHORT, Robert, Dunham, III** [US/US]; 38710 Goose Creek Lane, Leesburg, VA 20175 (US). **LARSON, Victor** [US/US]; 12026 Lisa Marie Court, Fairfax, VA 22033 (US). **WILLIAMSON, Michael** [US/US]; 26203 Ocala Circle, South Riding, VA 20152 (US).

(74) Agents: **WRIGHT, Bradley, C.** et al.; Banner & Witcoff, Ltd., 11th Floor, 1001 G Street, N.W., Washington, DC 20001-4597 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/61922 A2

(54) Title: IMPROVEMENTS TO AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY

(57) Abstract: A plurality of computer nodes communicate using seemingly random Internet Protocol source and destination addresses. Data packets matching criteria defined by a moving window of valid addresses are accepted for further processing, while those that do not meet the criteria are quickly rejected. Improvements to the basic design include (1) a load balancer that distributes packets across different transmission paths according to transmission path quality; (2) a DNS proxy server that transparently creates a virtual private network in response to a domain name inquiry; (3) a large-to-small link bandwidth management feature that prevents denial-of-service attacks at system chokepoints; (4) a traffic limit

IMPROVEMENTS TO AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY

CROSS-REFERENCE TO RELATED APPLICATION

This application claims priority from and is a continuation-in-part of previously filed U.S. application serial number 09/429,643, filed on October 29, 1999. The subject matter of that application, which is bodily incorporated herein, derives from provisional U.S. application numbers 60/106,261 (filed October 30, 1998) and 60/137,704 (filed June 7, 1999).

BACKGROUND OF THE INVENTION

A tremendous variety of methods have been proposed and implemented to provide security and anonymity for communications over the Internet. The variety stems, in part, from the different needs of different Internet users. A basic heuristic framework to aid in discussing these different security techniques is illustrated in FIG. 1. Two terminals, an originating terminal 100 and a destination terminal 110 are in communication over the Internet. It is desired for the communications to be secure, that is, immune to eavesdropping. For example, terminal 100 may transmit secret information to terminal 110 over the Internet 107. Also, it may be desired to prevent an eavesdropper from discovering that terminal 100 is in communication with terminal 110. For example, if terminal 100 is a user and terminal 110 hosts a web site, terminal 100's user may not want anyone in the intervening networks to know what web sites he is "visiting." Anonymity would thus be an issue, for example, for companies that want to keep their market research interests private and thus would prefer to prevent outsiders from knowing which web-sites or other Internet resources they are "visiting." These two security issues may be called data security and anonymity, respectively.

Data security is usually tackled using some form of data encryption. An encryption key 48 is known at both the originating and terminating terminals 100 and 110. The keys may be private and public at the originating and destination terminals 100 and 110, respectively or they may be symmetrical keys (the same key is used by

both parties to encrypt and decrypt). Many encryption methods are known and usable in this context.

To hide traffic from a local administrator or ISP, a user can employ a local proxy server in communicating over an encrypted channel with an outside proxy such that the local administrator or ISP only sees the encrypted traffic. Proxy servers prevent destination servers from determining the identities of the originating clients. This system employs an intermediate server interposed between client and destination server. The destination server sees only the Internet Protocol (IP) address of the proxy server and not the originating client. The target server only sees the address of the outside proxy. This scheme relies on a trusted outside proxy server. Also, proxy schemes are vulnerable to traffic analysis methods of determining identities of transmitters and receivers. Another important limitation of proxy servers is that the server knows the identities of both calling and called parties. In many instances, an originating terminal, such as terminal A, would prefer to keep its identity concealed from the proxy, for example, if the proxy server is provided by an Internet service provider (ISP).

To defeat traffic analysis, a scheme called Chaum's mixes employs a proxy server that transmits and receives fixed length messages, including dummy messages. Multiple originating terminals are connected through a mix (a server) to multiple target servers. It is difficult to tell which of the originating terminals are communicating to which of the connected target servers, and the dummy messages confuse eavesdroppers' efforts to detect communicating pairs by analyzing traffic. A drawback is that there is a risk that the mix server could be compromised. One way to deal with this risk is to spread the trust among multiple mixes. If one mix is compromised, the identities of the originating and target terminals may remain concealed. This strategy requires a number of alternative mixes so that the intermediate servers interposed between the originating and target terminals are not determinable except by compromising more than one mix. The strategy wraps the message with multiple layers of encrypted addresses. The first mix in a sequence can decrypt only the outer layer of the message to reveal the next destination mix in

sequence. The second mix can decrypt the message to reveal the next mix and so on. The target server receives the message and, optionally, a multi-layer encrypted payload containing return information to send data back in the same fashion. The only way to defeat such a mix scheme is to collude among mixes. If the packets are all fixed-length and intermixed with dummy packets, there is no way to do any kind of traffic analysis.

Still another anonymity technique, called 'crowds,' protects the identity of the originating terminal from the intermediate proxies by providing that originating terminals belong to groups of proxies called crowds. The crowd proxies are interposed between originating and target terminals. Each proxy through which the message is sent is randomly chosen by an upstream proxy. Each intermediate proxy can send the message either to another randomly chosen proxy in the "crowd" or to the destination. Thus, even crowd members cannot determine if a preceding proxy is the originator of the message or if it was simply passed from another proxy.

ZKS (Zero-Knowledge Systems) Anonymous IP Protocol allows users to select up to any of five different pseudonyms, while desktop software encrypts outgoing traffic and wraps it in User Datagram Protocol (UDP) packets. The first server in a 2+-hop system gets the UDP packets, strips off one layer of encryption to add another, then sends the traffic to the next server, which strips off yet another layer of encryption and adds a new one. The user is permitted to control the number of hops. At the final server, traffic is decrypted with an untraceable IP address. The technique is called onion-routing. This method can be defeated using traffic analysis. For a simple example, bursts of packets from a user during low-duty periods can reveal the identities of sender and receiver.

Firewalls attempt to protect LANs from unauthorized access and hostile exploitation or damage to computers connected to the LAN. Firewalls provide a server through which all access to the LAN must pass. Firewalls are centralized systems that require administrative overhead to maintain. They can be compromised by virtual-machine applications ("applets"). They instill a false sense of security that leads to security breaches for example by users sending sensitive information to

servers outside the firewall or encouraging use of modems to sidestep the firewall security. Firewalls are not useful for distributed systems such as business travelers, extranets, small teams, etc.

SUMMARY OF THE INVENTION

A secure mechanism for communicating over the internet, including a protocol referred to as the Tunneled Agile Routing Protocol (TARP), uses a unique two-layer encryption format and special TARP routers. TARP routers are similar in function to regular IP routers. Each TARP router has one or more IP addresses and uses normal IP protocol to send IP packet messages ("packets" or "datagrams"). The IP packets exchanged between TARP terminals via TARP routers are actually encrypted packets whose true destination address is concealed except to TARP routers and servers. The normal or "clear" or "outside" IP header attached to TARP IP packets contains only the address of a next hop router or destination server. That is, instead of indicating a final destination in the destination field of the IP header, the TARP packet's IP header always points to a next-hop in a series of TARP router hops, or to the final destination. This means there is no overt indication from an intercepted TARP packet of the true destination of the TARP packet since the destination could always be next-hop TARP router as well as the final destination.

Each TARP packet's true destination is concealed behind a layer of encryption generated using a link key. The link key is the encryption key used for encrypted communication between the hops intervening between an originating TARP terminal and a destination TARP terminal. Each TARP router can remove the outer layer of encryption to reveal the destination router for each TARP packet. To identify the link key needed to decrypt the outer layer of encryption of a TARP packet, a receiving TARP or routing terminal may identify the transmitting terminal by the sender/receiver IP numbers in the cleartext IP header.

Once the outer layer of encryption is removed, the TARP router determines the final destination. Each TARP packet 140 undergoes a minimum number of hops to help foil traffic analysis. The hops may be chosen at random or by a fixed value. As a result, each TARP packet may make random trips among a number of geographically

disparate routers before reaching its destination. Each trip is highly likely to be different for each packet composing a given message because each trip is independently randomly determined. This feature is called *agile routing*. The fact that different packets take different routes provides distinct advantages by making it difficult for an interloper to obtain all the packets forming an entire multi-packet message. The associated advantages have to do with the inner layer of encryption discussed below. Agile routing is combined with another feature that furthers this purpose; a feature that ensures that any message is broken into multiple packets.

The IP address of a TARP router can be changed, a feature called *IP agility*. Each TARP router, independently or under direction from another TARP terminal or router, can change its IP address. A separate, unchangeable identifier or address is also defined. This address, called the TARP address, is known only to TARP routers and terminals and may be correlated at any time by a TARP router or a TARP terminal using a Lookup Table (LUT). When a TARP router or terminal changes its IP address, it updates the other TARP routers and terminals which in turn update their respective LUTs.

The message payload is hidden behind an inner layer of encryption in the TARP packet that can only be unlocked using a session key. The session key is not available to any of the intervening TARP routers. The session key is used to decrypt the payloads of the TARP packets permitting the data stream to be reconstructed.

Communication may be made private using link and session keys, which in turn may be shared and used according to any desired method. For example, public/private keys or symmetric keys may be used.

To transmit a data stream, a TARP originating terminal constructs a series of TARP packets from a series of IP packets generated by a network (IP) layer process. (Note that the terms "network layer," "data link layer," "application layer," etc. used in this specification correspond to the Open Systems Interconnection (OSI) network terminology.) The payloads of these packets are assembled into a block and chain-block encrypted using the session key. This assumes, of course, that all the IP packets are destined for the same TARP terminal. The block is then interleaved and the

interleaved encrypted block is broken into a series of payloads, one for each TARP packet to be generated. Special TARP headers IP_T are then added to each payload using the IP headers from the data stream packets. The TARP headers can be identical to normal IP headers or customized in some way. They should contain a formula or data for deinterleaving the data at the destination TARP terminal, a time-to-live (TTL) parameter to indicate the number of hops still to be executed, a data type identifier which indicates whether the payload contains, for example, TCP or UDP data, the sender's TARP address, the destination TARP address, and an indicator as to whether the packet contains real or decoy data or a formula for filtering out decoy data if decoy data is spread in some way through the TARP payload data.

Note that although chain-block encryption is discussed here with reference to the session key, any encryption method may be used. Preferably, as in chain block encryption, a method should be used that makes unauthorized decryption difficult without an entire result of the encryption process. Thus, by separating the encrypted block among multiple packets and making it difficult for an interloper to obtain access to all of such packets, the contents of the communications are provided an extra layer of security.

Decoy or dummy data can be added to a stream to help foil traffic analysis by reducing the peak-to-average network load. It may be desirable to provide the TARP process with an ability to respond to the time of day or other criteria to generate more decoy data during low traffic periods so that communication bursts at one point in the Internet cannot be tied to communication bursts at another point to reveal the communicating endpoints.

Dummy data also helps to break the data into a larger number of inconspicuously-sized packets permitting the interleave window size to be increased while maintaining a reasonable size for each packet. (The packet size can be a single standard size or selected from a fixed range of sizes.) One primary reason for desiring for each message to be broken into multiple packets is apparent if a chain block encryption scheme is used to form the first encryption layer prior to interleaving. A single block encryption may be applied to portion, or entirety, of a message, and that

portion or entirety then interleaved into a number of separate packets. Considering the agile IP routing of the packets, and the attendant difficulty of reconstructing an entire sequence of packets to form a single block-encrypted message element, decoy packets can significantly increase the difficulty of reconstructing an entire data stream.

The above scheme may be implemented entirely by processes operating between the data link layer and the network layer of each server or terminal participating in the TARP system. Because the encryption system described above is insertable between the data link and network layers, the processes involved in supporting the encrypted communication may be completely transparent to processes at the IP (network) layer and above. The TARP processes may also be completely transparent to the data link layer processes as well. Thus, no operations at or above the Network layer, or at or below the data link layer, are affected by the insertion of the TARP stack. This provides additional security to all processes at or above the network layer, since the difficulty of unauthorized penetration of the network layer (by, for example, a hacker) is increased substantially. Even newly developed servers running at the session layer leave all processes below the session layer vulnerable to attack. Note that in this architecture, security is distributed. That is, notebook computers used by executives on the road, for example, can communicate over the Internet without any compromise in security.

IP address changes made by TARP terminals and routers can be done at regular intervals, at random intervals, or upon detection of "attacks." The variation of IP addresses hinders traffic analysis that might reveal which computers are communicating, and also provides a degree of immunity from attack. The level of immunity from attack is roughly proportional to the rate at which the IP address of the host is changing.

As mentioned, IP addresses may be changed in response to attacks. An attack may be revealed, for example, by a regular series of messages indicating that a router is being probed in some way. Upon detection of an attack, the TARP layer process may respond to this event by changing its IP address. In addition, it may create a

subprocess that maintains the original IP address and continues interacting with the attacker in some manner.

Decoy packets may be generated by each TARP terminal on some basis determined by an algorithm. For example, the algorithm may be a random one which calls for the generation of a packet on a random basis when the terminal is idle. Alternatively, the algorithm may be responsive to time of day or detection of low traffic to generate more decoy packets during low traffic times. Note that packets are preferably generated in groups, rather than one by one, the groups being sized to simulate real messages. In addition, so that decoy packets may be inserted in normal TARP message streams, the background loop may have a latch that makes it more likely to insert decoy packets when a message stream is being received. Alternatively, if a large number of decoy packets is received along with regular TARP packets, the algorithm may increase the rate of dropping of decoy packets rather than forwarding them. The result of dropping and generating decoy packets in this way is to make the apparent incoming message size different from the apparent outgoing message size to help foil traffic analysis.

In various other embodiments of the invention, a scalable version of the system may be constructed in which a plurality of IP addresses are preassigned to each pair of communicating nodes in the network. Each pair of nodes agrees upon an algorithm for "hopping" between IP addresses (both sending and receiving), such that an eavesdropper sees apparently continuously random IP address pairs (source and destination) for packets transmitted between the pair. Overlapping or "reusable" IP addresses may be allocated to different users on the same subnet, since each node merely verifies that a particular packet includes a valid source/destination pair from the agreed-upon algorithm. Source/destination pairs are preferably not reused between any two nodes during any given end-to-end session, though limited IP block sizes or lengthy sessions might require it.

Further improvements described in this continuation-in-part application include: (1) a load balancer that distributes packets across different transmission paths according to transmission path quality; (2) a DNS proxy server that transparently

creates a virtual private network in response to a domain name inquiry; (3) a large-to-small link bandwidth management feature that prevents denial-of-service attacks at system chokepoints; (4) a traffic limiter that regulates incoming packets by limiting the rate at which a transmitter can be synchronized with a receiver; and (5) a signaling synchronizer that allows a large number of nodes to communicate with a central node by partitioning the communication function between two separate entities

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is an illustration of secure communications over the Internet according to a prior art embodiment.

FIG. 2 is an illustration of secure communications over the Internet according to a an embodiment of the invention.

FIG. 3a is an illustration of a process of forming a tunneled IP packet according to an embodiment of the invention.

FIG. 3b is an illustration of a process of forming a tunneled IP packet according to another embodiment of the invention.

FIG. 4 is an illustration of an OSI layer location of processes that may be used to implement the invention.

FIG. 5 is a flow chart illustrating a process for routing a tunneled packet according to an embodiment of the invention.

FIG. 6 is a flow chart illustrating a process for forming a tunneled packet according to an embodiment of the invention.

FIG. 7 is a flow chart illustrating a process for receiving a tunneled packet according to an embodiment of the invention.

FIG. 8 shows how a secure session is established and synchronized between a client and a TARP router.

FIG. 9 shows an IP address hopping scheme between a client computer and TARP router using transmit and receive tables in each computer.

FIG. 10 shows physical link redundancy among three Internet Service Providers (ISPs) and a client computer.

FIG. 11 shows how multiple IP packets can be embedded into a single "frame" such as an Ethernet frame, and further shows the use of a discriminator field to camouflage true packet recipients.

FIG. 12A shows a system that employs hopped hardware addresses, hopped IP addresses, and hopped discriminator fields.

FIG. 12B shows several different approaches for hopping hardware addresses, IP addresses, and discriminator fields in combination.

FIG. 13 shows a technique for automatically re-establishing synchronization between sender and receiver through the use of a partially public sync value.

FIG. 14 shows a "checkpoint" scheme for regaining synchronization between a sender and recipient.

FIG. 15 shows further details of the checkpoint scheme of FIG. 14.

FIG. 16 shows how two addresses can be decomposed into a plurality of segments for comparison with presence vectors.

FIG. 17 shows a storage array for a receiver's active addresses.

FIG. 18 shows the receiver's storage array after receiving a sync request.

FIG. 19 shows the receiver's storage array after new addresses have been generated.

FIG. 20 shows a system employing distributed transmission paths.

FIG. 21 shows a plurality of link transmission tables that can be used to route packets in the system of FIG. 20.

FIG. 22A shows a flowchart for adjusting weight value distributions associated with a plurality of transmission links.

FIG. 22B shows a flowchart for setting a weight value to zero if a transmitter turns off.

FIG. 23 shows a system employing distributed transmission paths with adjusted weight value distributions for each path.

FIG. 24 shows an example using the system of FIG. 23.

FIG. 25 shows a conventional domain-name look-up service.

FIG. 26 shows a system employing a DNS proxy server with transparent VPN creation.

FIG. 27 shows steps that can be carried out to implement transparent VPN creation based on a DNS look-up function.

FIG. 28 shows a system including a link guard function that prevents packet overloading on a low-bandwidth link LOW BW.

FIG. 29 shows one embodiment of a system employing the principles of FIG. 28.

FIG. 30 shows a system that regulates packet transmission rates by throttling the rate at which synchronizations are performed.

FIG. 31 shows a signaling server 3101 and a transport server 3102 used to establish a VPN with a client computer.

FIG. 32 shows message flows relating to synchronization protocols of FIG. 31.

DETAILED DESCRIPTION OF THE INVENTION

Referring to FIG. 2, a secure mechanism for communicating over the internet employs a number of special routers or servers, called TARP routers 122-127 that are similar to regular IP routers 128-132 in that each has one or more IP addresses and uses normal IP protocol to send normal-looking IP packet messages, called TARP packets 140. TARP packets 140 are identical to normal IP packet messages that are routed by regular IP routers 128-132 because each TARP packet 140 contains a destination address as in a normal IP packet. However, instead of indicating a final destination in the destination field of the IP header, the TARP packet's 140 IP header always points to a next-hop in a series of TARP router hops, or the final destination, TARP terminal 110. Because the header of the TARP packet contains only the next-hop destination, there is no overt indication from an intercepted TARP packet of the true destination of the TARP packet 140 since the destination could always be the next-hop TARP router as well as the final destination, TARP terminal 110.

Each TARP packet's true destination is concealed behind an outer layer of encryption generated using a link key 146. The link key 146 is the encryption key used for encrypted communication between the end points (TARP terminals or TARP

routers) of a single link in the chain of hops connecting the originating TARP terminal 100 and the destination TARP terminal 110. Each TARP router 122-127, using the link key 146 it uses to communicate with the previous hop in a chain, can use the link key to reveal the true destination of a TARP packet. To identify the link key needed to decrypt the outer layer of encryption of a TARP packet, a receiving TARP or routing terminal may identify the transmitting terminal (which may indicate the link key used) by the sender field of the clear IP header. Alternatively, this identity may be hidden behind another layer of encryption in available bits in the clear IP header. Each TARP router, upon receiving a TARP message, determines if the message is a TARP message by using authentication data in the TARP packet. This could be recorded in available bytes in the TARP packet's IP header. Alternatively, TARP packets could be authenticated by attempting to decrypt using the link key 146 and determining if the results are as expected. The former may have computational advantages because it does not involve a decryption process.

Once the outer layer of decryption is completed by a TARP router 122-127, the TARP router determines the final destination. The system is preferably designed to cause each TARP packet 140 to undergo a minimum number of hops to help foil traffic analysis. The time to live counter in the IP header of the TARP message may be used to indicate a number of TARP router hops yet to be completed. Each TARP router then would decrement the counter and determine from that whether it should forward the TARP packet 140 to another TARP router 122-127 or to the destination TARP terminal 110. If the time to live counter is zero or below zero after decrementing, for an example of usage, the TARP router receiving the TARP packet 140 may forward the TARP packet 140 to the destination TARP terminal 110. If the time to live counter is above zero after decrementing, for an example of usage, the TARP router receiving the TARP packet 140 may forward the TARP packet 140 to a TARP router 122-127 that the current TARP terminal chooses at random. As a result, each TARP packet 140 is routed through some minimum number of hops of TARP routers 122-127 which are chosen at random.

Thus, each TARP packet, irrespective of the traditional factors determining traffic in the Internet, makes random trips among a number of geographically disparate routers before reaching its destination and each trip is highly likely to be different for each packet composing a given message because each trip is independently randomly determined as described above. This feature is called *agile routing*. For reasons that will become clear shortly, the fact that different packets take different routes provides distinct advantages by making it difficult for an interloper to obtain all the packets forming an entire multi-packet message. Agile routing is combined with another feature that furthers this purpose, a feature that ensures that any message is broken into multiple packets.

A TARP router receives a TARP packet when an IP address used by the TARP router coincides with the IP address in the TARP packet's IP header IP_C. The IP address of a TARP router, however, may not remain constant. To avoid and manage attacks, each TARP router, independently or under direction from another TARP terminal or router, may change its IP address. A separate, unchangeable identifier or address is also defined. This address, called the TARP address, is known only to TARP routers and terminals and may be correlated at any time by a TARP router or a TARP terminal using a Lookup Table (LUT). When a TARP router or terminal changes its IP address, it updates the other TARP routers and terminals which in turn update their respective LUTs. In reality, whenever a TARP router looks up the address of a destination in the encrypted header, it must convert a TARP address to a real IP address using its LUT.

While every TARP router receiving a TARP packet has the ability to determine the packet's final destination, the message payload is embedded behind an inner layer of encryption in the TARP packet that can only be unlocked using a session key. The session key is not available to any of the TARP routers 122-127 intervening between the originating 100 and destination 110 TARP terminals. The session key is used to decrypt the payloads of the TARP packets 140 permitting an entire message to be reconstructed.

In one embodiment, communication may be made private using link and session keys, which in turn may be shared and used according any desired method. For example, a public key or symmetric keys may be communicated between link or session endpoints using a public key method. Any of a variety of other mechanisms for securing data to ensure that only authorized computers can have access to the private information in the TARP packets 140 may be used as desired.

Referring to FIG. 3a, to construct a series of TARP packets, a data stream 300 of IP packets 207a, 207b, 207c, etc., such series of packets being formed by a network (IP) layer process, is broken into a series of small sized segments. In the present example, equal-sized segments 1-9 are defined and used to construct a set of interleaved data packets A, B, and C. Here it is assumed that the number of interleaved packets A, B, and C formed is three and that the number of IP packets 207a-207c used to form the three interleaved packets A, B, and C is exactly three. Of course, the number of IP packets spread over a group of interleaved packets may be any convenient number as may be the number of interleaved packets over which the incoming data stream is spread. The latter, the number of interleaved packets over which the data stream is spread, is called the *interleave window*.

To create a packet, the transmitting software interleaves the normal IP packets 207a *et. seq.* to form a new set of interleaved payload data 320. This payload data 320 is then encrypted using a session key to form a set of session-key-encrypted payload data 330, each of which, A, B, and C, will form the payload of a TARP packet. Using the IP header data, from the original packets 207a-207c, new TARP headers IP_T are formed. The TARP headers IP_T can be identical to normal IP headers or customized in some way. In a preferred embodiment, the TARP headers IP_T are IP headers with added data providing the following information required for routing and reconstruction of messages, some of which data is ordinarily, or capable of being, contained in normal IP headers:

1. A window sequence number – an identifier that indicates where the packet belongs in the original message sequence.

2. An interleave sequence number – an identifier that indicates the interleaving sequence used to form the packet so that the packet can be deinterleaved along with other packets in the interleave window.

3. A time-to-live (TTL) datum – indicates the number of TARP-router-hops to be executed before the packet reaches its destination. Note that the TTL parameter may provide a datum to be used in a probabilistic formula for determining whether to route the packet to the destination or to another hop.

4. Data type identifier – indicates whether the payload contains, for example, TCP or UDP data.

5. Sender's address – indicates the sender's address in the TARP network.

6. Destination address – indicates the destination terminal's address in the TARP network.

7. Decoy/Real – an indicator of whether the packet contains real message data or dummy decoy data or a combination.

Obviously, the packets going into a single interleave window must include only packets with a common destination. Thus, it is assumed in the depicted example that the IP headers of IP packets 207a-207c all contain the same destination address or at least will be received by the same terminal so that they can be deinterleaved. Note that dummy or decoy data or packets can be added to form a larger interleave window than would otherwise be required by the size of a given message. Decoy or dummy data can be added to a stream to help foil traffic analysis by leveling the load on the network. Thus, it may be desirable to provide the TARP process with an ability to respond to the time of day or other criteria to generate more decoy data during low traffic periods so that communication bursts at one point in the Internet cannot be tied to communication bursts at another point to reveal the communicating endpoints.

Dummy data also helps to break the data into a larger number of inconspicuously-sized packets permitting the interleave window size to be increased while maintaining a reasonable size for each packet. (The packet size can be a single

standard size or selected from a fixed range of sizes.) One primary reason for desiring for each message to be broken into multiple packets is apparent if a chain block encryption scheme is used to form the first encryption layer prior to interleaving. A single block encryption may be applied to a portion, or the entirety, of a message, and that portion or entirety then interleaved into a number of separate packets.

Referring to FIG. 3b, in an alternative mode of TARP packet construction, a series of IP packets are accumulated to make up a predefined interleave window. The payloads of the packets are used to construct a single block 520 for chain block encryption using the session key. The payloads used to form the block are presumed to be destined for the same terminal. The block size may coincide with the interleave window as depicted in the example embodiment of FIG. 3b. After encryption, the encrypted block is broken into separate payloads and segments which are interleaved as in the embodiment of Fig 3a. The resulting interleaved packets A, B, and C, are then packaged as TARP packets with TARP headers as in the Example of FIG. 3a. The remaining process is as shown in, and discussed with reference to, FIG. 3a.

Once the TARP packets 340 are formed, each entire TARP packet 340, including the TARP header IP_T, is encrypted using the link key for communication with the first-hop-TARP router. The first hop TARP router is randomly chosen. A final unencrypted IP header IP_C is added to each encrypted TARP packet 340 to form a normal IP packet 360 that can be transmitted to a TARP router. Note that the process of constructing the TARP packet 360 does not have to be done in stages as described. The above description is just a useful heuristic for describing the final product, namely, the TARP packet.

Note that, TARP header IP_T could be a completely custom header configuration with no similarity to a normal IP header except that it contain the information identified above. This is so since this header is interpreted by only TARP routers.

The above scheme may be implemented entirely by processes operating between the data link layer and the network layer of each server or terminal participating in the TARP system. Referring to FIG. 4, a TARP transceiver 405 can be

an originating terminal 100, a destination terminal 110, or a TARP router 122-127. In each TARP Transceiver 405, a transmitting process is generated to receive normal packets from the Network (IP) layer and generate TARP packets for communication over the network. A receiving process is generated to receive normal IP packets containing TARP packets and generate from these normal IP packets which are "passed up" to the Network (IP) layer. Note that where the TARP Transceiver 405 is a router, the received TARP packets 140 are not processed into a stream of IP packets 415 because they need only be authenticated as proper TARP packets and then passed to another TARP router or a TARP destination terminal 110. The intervening process, a "TARP Layer" 420, could be combined with either the data link layer 430 or the Network layer 410. In either case, it would intervene between the data link layer 430 so that the process would receive regular IP packets containing embedded TARP packets and "hand up" a series of reassembled IP packets to the Network layer 410. As an example of combining the TARP layer 420 with the data link layer 430, a program may augment the normal processes running a communications card, for example, an Ethernet card. Alternatively, the TARP layer processes may form part of a dynamically loadable module that is loaded and executed to support communications between the network and data link layers.

Because the encryption system described above can be inserted between the data link and network layers, the processes involved in supporting the encrypted communication may be completely transparent to processes at the IP (network) layer and above. The TARP processes may also be completely transparent to the data link layer processes as well. Thus, no operations at or above the network layer, or at or below the data link layer, are affected by the insertion of the TARP stack. This provides additional security to all processes at or above the network layer, since the difficulty of unauthorized penetration of the network layer (by, for example, a hacker) is increased substantially. Even newly developed servers running at the session layer leave all processes below the session layer vulnerable to attack. Note that in this architecture, security is distributed. That is, notebook computers used by executives

on the road, for example, can communicate over the Internet without any compromise in security.

Note that IP address changes made by TARP terminals and routers can be done at regular intervals, at random intervals, or upon detection of "attacks." The variation of IP addresses hinders traffic analysis that might reveal which computers are communicating, and also provides a degree of immunity from attack. The level of immunity from attack is roughly proportional to the rate at which the IP address of the host is changing.

As mentioned, IP addresses may be changed in response to attacks. An attack may be revealed, for example, by a regular series of messages indicates that a router is being probed in some way. Upon detection of an attack, the TARP layer process may respond to this event by changing its IP address. To accomplish this, the TARP process will construct a TARP-formatted message, in the style of Internet Control Message Protocol (ICMP) datagrams as an example; this message will contain the machine's TARP address, its previous IP address, and its new IP address. The TARP layer will transmit this packet to at least one known TARP router; then upon receipt and validation of the message, the TARP router will update its LUT with the new IP address for the stated TARP address. The TARP router will then format a similar message, and broadcast it to the other TARP routers so that they may update their LUTs. Since the total number of TARP routers on any given subnet is expected to be relatively small, this process of updating the LUTs should be relatively fast. It may not, however, work as well when there is a relatively large number of TARP routers and/or a relatively large number of clients; this has motivated a refinement of this architecture to provide scalability; this refinement has led to a second embodiment, which is discussed below.

Upon detection of an attack, the TARP process may also create a subprocess that maintains the original IP address and continues interacting with the attacker. The latter may provide an opportunity to trace the attacker or study the attacker's methods (called "fishbowling" drawing upon the analogy of a small fish in a fish bowl that "thinks" it is in the ocean but is actually under captive observation). A history of the

communication between the attacker and the abandoned (fishbowled) IP address can be recorded or transmitted for human analysis or further synthesized for purposes of responding in some way.

As mentioned above, decoy or dummy data or packets can be added to outgoing data streams by TARP terminals or routers. In addition to making it convenient to spread data over a larger number of separate packets, such decoy packets can also help to level the load on inactive portions of the Internet to help foil traffic analysis efforts.

Decoy packets may be generated by each TARP terminal 100, 110 or each router 122-127 on some basis determined by an algorithm. For example, the algorithm may be a random one which calls for the generation of a packet on a random basis when the terminal is idle. Alternatively, the algorithm may be responsive to time of day or detection of low traffic to generate more decoy packets during low traffic times. Note that packets are preferably generated in groups, rather than one by one, the groups being sized to simulate real messages. In addition, so that decoy packets may be inserted in normal TARP message streams, the background loop may have a latch that makes it more likely to insert decoy packets when a message stream is being received. That is, when a series of messages are received, the decoy packet generation rate may be increased. Alternatively, if a large number of decoy packets is received along with regular TARP packets, the algorithm may increase the rate of dropping of decoy packets rather than forwarding them. The result of dropping and generating decoy packets in this way is to make the apparent incoming message size different from the apparent outgoing message size to help foil traffic analysis. The rate of reception of packets, decoy or otherwise, may be indicated to the decoy packet dropping and generating processes through perishable decoy and regular packet counters. (A perishable counter is one that resets or decrements its value in response to time so that it contains a high value when it is incremented in rapid succession and a small value when incremented either slowly or a small number of times in rapid succession.) Note that destination TARP terminal 110 may generate decoy packets

equal in number and size to those TARP packets received to make it appear it is merely routing packets and is therefore not the destination terminal.

Referring to FIG. 5, the following particular steps may be employed in the above-described method for routing TARP packets.

- S0. A background loop operation is performed which applies an algorithm which determines the generation of decoy IP packets. The loop is interrupted when an encrypted TARP packet is received.
- S2. The TARP packet may be probed in some way to authenticate the packet before attempting to decrypt it using the link key. That is, the router may determine that the packet is an authentic TARP packet by performing a selected operation on some data included with the clear IP header attached to the encrypted TARP packet contained in the payload. This makes it possible to avoid performing decryption on packets that are not authentic TARP packets.
- S3. The TARP packet is decrypted to expose the destination TARP address and an indication of whether the packet is a decoy packet or part of a real message.
- S4. If the packet is a decoy packet, the perishable decoy counter is incremented.
- S5. Based on the decoy generation/dropping algorithm and the perishable decoy counter value, if the packet is a decoy packet, the router may choose to throw it away. If the received packet is a decoy packet and it is determined that it should be thrown away (S6), control returns to step S0.
- S7. The TTL parameter of the TARP header is decremented and it is determined if the TTL parameter is greater than zero.
- S8. If the TTL parameter is greater than zero, a TARP address is randomly chosen from a list of TARP addresses maintained by the router and the link key and IP address corresponding to that TARP address memorized for use in creating a new IP packet containing the TARP packet.
- S9. If the TTL parameter is zero or less, the link key and IP address corresponding to the TARP address of the destination are memorized for use in creating the new IP packet containing the TARP packet.

- S10. The TARP packet is encrypted using the memorized link key.
- S11. An IP header is added to the packet that contains the stored IP address, the encrypted TARP packet wrapped with an IP header. and the completed packet transmitted to the next hop or destination.

Referring to FIG. 6. the following particular steps may be employed in the above-described method for generating TARP packets.

- S20. A background loop operation applies an algorithm that determines the generation of decoy IP packets. The loop is interrupted when a data stream containing IP packets is received for transmission.
- S21. The received IP packets are grouped into a set consisting of messages with a constant IP destination address. The set is further broken down to coincide with a maximum size of an interleave window The set is encrypted. and interleaved into a set of payloads destined to become TARP packets.
- S22. The TARP address corresponding to the IP address is determined from a lookup table and stored to generate the TARP header. An initial TTL count is generated and stored in the header. The TTL count may be random with minimum and maximum values or it may be fixed or determined by some other parameter.
- S23. The window sequence numbers and interleave sequence numbers are recorded in the TARP headers of each packet.
- S24. One TARP router address is randomly chosen for each TARP packet and the IP address corresponding to it stored for use in the clear IP header. The link key corresponding to this router is identified and used to encrypt TARP packets containing interleaved and encrypted data and TARP headers.
- S25. A clear IP header with the first hop router's real IP address is generated and added to each of the encrypted TARP packets and the resulting packets.

Referring to FIG. 7. the following particular steps may be employed in the above-described method for receiving TARP packets.

- S40. A background loop operation is performed which applies an algorithm which determines the generation of decoy IP packets. The loop is interrupted when an encrypted TARP packet is received.
- S42. The TARP packet may be probed to authenticate the packet before attempting to decrypt it using the link key.
- S43. The TARP packet is decrypted with the appropriate link key to expose the destination TARP address and an indication of whether the packet is a decoy packet or part of a real message.
- S44. If the packet is a decoy packet, the perishable decoy counter is incremented.
- S45. Based on the decoy generation/dropping algorithm and the perishable decoy counter value, if the packet is a decoy packet, the receiver may choose to throw it away.
- S46. The TARP packets are cached until all packets forming an interleave window are received.
- S47. Once all packets of an interleave window are received, the packets are deinterleaved.
- S48. The packets block of combined packets defining the interleave window is then decrypted using the session key.
- S49. The decrypted block is then divided using the window sequence data and the IP_T headers are converted into normal IP_C headers. The window sequence numbers are integrated in the IP_C headers.
- S50. The packets are then handed up to the IP layer processes.

1. SCALABILITY ENHANCEMENTS

The IP agility feature described above relies on the ability to transmit IP address changes to all TARP routers. The embodiments including this feature will be referred to as "boutique" embodiments due to potential limitations in scaling these features up for a large network, such as the Internet. (The "boutique" embodiments would, however, be robust for use in smaller networks, such as small virtual private networks, for example). One problem with the boutique embodiments is that if IP

address changes are to occur frequently, the message traffic required to update all routers sufficiently quickly creates a serious burden on the Internet when the TARP router and/or client population gets large. The bandwidth burden added to the networks, for example in ICMP packets, that would be used to update all the TARP routers could overwhelm the Internet for a large scale implementation that approached the scale of the Internet. In other words, the boutique system's scalability is limited.

A system can be constructed which trades some of the features of the above embodiments to provide the benefits of IP agility without the additional messaging burden. This is accomplished by IP address-hopping according to shared algorithms that govern IP addresses used between links participating in communications sessions between nodes such as TARP nodes. (Note that the IP hopping technique is also applicable to the boutique embodiment.) The IP agility feature discussed with respect to the boutique system can be modified so that it becomes decentralized under this scalable regime and governed by the above-described shared algorithm. Other features of the boutique system may be combined with this new type of IP-agility.

The new embodiment has the advantage of providing IP agility governed by a local algorithm and set of IP addresses exchanged by each communicating pair of nodes. This local governance is session-independent in that it may govern communications between a pair of nodes, irrespective of the session or end points being transferred between the directly communicating pair of nodes.

In the scalable embodiments, blocks of IP addresses are allocated to each node in the network. (This scalability will increase in the future, when Internet Protocol addresses are increased to 128-bit fields, vastly increasing the number of distinctly addressable nodes). Each node can thus use any of the IP addresses assigned to that node to communicate with other nodes in the network. Indeed, each pair of communicating nodes can use a plurality of source IP addresses and destination IP addresses for communicating with each other.

Each communicating pair of nodes in a chain participating in any session stores two blocks of IP addresses, called netblocks, and an algorithm and randomization seed for selecting, from each netblock, the next pair of

source/destination IP addresses that will be used to transmit the next message. In other words, the algorithm governs the sequential selection of IP-address pairs, one sender and one receiver IP address, from each netblock. The combination of algorithm, seed, and netblock (IP address block) will be called a "hopblock." A router issues separate transmit and receive hopblocks to its clients. The send address and the receive address of the IP header of each outgoing packet sent by the client are filled with the send and receive IP addresses generated by the algorithm. The algorithm is "clocked" (indexed) by a counter so that each time a pair is used, the algorithm turns out a new transmit pair for the next packet to be sent.

The router's receive hopblock is identical to the client's transmit hopblock. The router uses the receive hopblock to predict what the send and receive IP address pair for the next expected packet from that client will be. Since packets can be received out of order, it is not possible for the router to predict with certainty what IP address pair will be on the next sequential packet. To account for this problem, the router generates a range of predictions encompassing the number of possible transmitted packet send/receive addresses, of which the next packet received could leap ahead. Thus, if there is a vanishingly small probability that a given packet will arrive at the router ahead of 5 packets transmitted by the client before the given packet, then the router can generate a series of 6 send/receive IP address pairs (or "hop window") to compare with the next received packet. When a packet is received, it is marked in the hop window as such, so that a second packet with the same IP address pair will be discarded. If an out-of-sequence packet does not arrive within a predetermined timeout period, it can be requested for retransmission or simply discarded from the receive table, depending upon the protocol in use for that communications session, or possibly by convention.

When the router receives the client's packet, it compares the send and receive IP addresses of the packet with the next N predicted send and receive IP address pairs and rejects the packet if it is not a member of this set. Received packets that do not have the predicted source/destination IP addresses falling with the window are rejected, thus thwarting possible hackers. (With the number of possible combinations,

even a fairly large window would be hard to fall into at random.) If it is a member of this set, the router accepts the packet and processes it further. This link-based IP-hopping strategy, referred to as "IHOP," is a network element that stands on its own and is not necessarily accompanied by elements of the boutique system described above. If the routing agility feature described in connection with the boutique embodiment is combined with this link-based IP-hopping strategy, the router's next step would be to decrypt the TARP header to determine the destination TARP router for the packet and determine what should be the next hop for the packet. The TARP router would then forward the packet to a random TARP router or the destination TARP router with which the source TARP router has a link-based IP hopping communication established.

Figure 8 shows how a client computer 801 and a TARP router 811 can establish a secure session. When client 801 seeks to establish an IHOP session with TARP router 811, the client 801 sends "secure synchronization" request ("SSYN") packet 821 to the TARP router 811. This SYN packet 821 contains the client's 801 authentication token, and may be sent to the router 811 in an encrypted format. The source and destination IP numbers on the packet 821 are the client's 801 current fixed IP address, and a "known" fixed IP address for the router 811. (For security purposes, it may be desirable to reject any packets from outside of the local network that are destined for the router's known fixed IP address.) Upon receipt and validation of the client's 801 SSYN packet 821, the router 811 responds by sending an encrypted "secure synchronization acknowledgment" ("SSYN ACK") 822 to the client 801. This SSYN ACK 822 will contain the transmit and receive hopblocks that the client 801 will use when communicating with the TARP router 811. The client 801 will acknowledge the TARP router's 811 response packet 822 by generating an encrypted SSYN ACK ACK packet 823 which will be sent from the client's 801 fixed IP address and to the TARP router's 811 known fixed IP address. The client 801 will simultaneously generate a SSYN ACK ACK packet; this SSYN ACK packet, referred to as the Secure Session Initiation (SSI) packet 824, will be sent with the first {sender, receiver} IP pair in the client's transmit table 921 (FIG. 9), as specified in the

transmit hopblock provided by the TARP router 811 in the SSYN ACK packet 822. The TARP router 811 will respond to the SSI packet 824 with an SSI ACK packet 825, which will be sent with the first {sender, receiver} IP pair in the TARP router's transmit table 923. Once these packets have been successfully exchanged, the secure communications session is established, and all further secure communications between the client 801 and the TARP router 811 will be conducted via this secure session, as long as synchronization is maintained. If synchronization is lost, then the client 801 and TARP router 802 may re-establish the secure session by the procedure outlined in Figure 8 and described above.

While the secure session is active, both the client 901 and TARP router 911 (FIG. 9) will maintain their respective transmit tables 921, 923 and receive tables 922, 924, as provided by the TARP router during session synchronization 822. It is important that the sequence of IP pairs in the client's transmit table 921 be identical to those in the TARP router's receive table 924; similarly, the sequence of IP pairs in the client's receive table 922 must be identical to those in the router's transmit table 923. This is required for the session synchronization to be maintained. The client 901 need maintain only one transmit table 921 and one receive table 922 during the course of the secure session. Each sequential packet sent by the client 901 will employ the next {send, receive} IP address pair in the transmit table, regardless of TCP or UDP session. The TARP router 911 will expect each packet arriving from the client 901 to bear the next IP address pair shown in its receive table.

Since packets can arrive out of order, however, the router 911 can maintain a "look ahead" buffer in its receive table, and will mark previously-received IP pairs as invalid for future packets; any future packet containing an IP pair that is in the look-ahead buffer but is marked as previously received will be discarded. Communications from the TARP router 911 to the client 901 are maintained in an identical manner; in particular, the router 911 will select the next IP address pair from its transmit table 923 when constructing a packet to send to the client 901, and the client 901 will maintain a look-ahead buffer of expected IP pairs on packets that it is receiving. Each

TARP router will maintain separate pairs of transmit and receive tables for each client that is currently engaged in a secure session with or through that TARP router.

While clients receive their hopblocks from the first server linking them to the Internet, routers exchange hopblocks. When a router establishes a link-based IP-hopping communication regime with another router, each router of the pair exchanges its transmit hopblock. The transmit hopblock of each router becomes the receive hopblock of the other router. The communication between routers is governed as described by the example of a client sending a packet to the first router.

While the above strategy works fine in the IP milieu, many local networks that are connected to the Internet are Ethernet systems. In Ethernet, the IP addresses of the destination devices must be translated into hardware addresses, and vice versa, using known processes ("address resolution protocol," and "reverse address resolution protocol"). However, if the link-based IP-hopping strategy is employed, the correlation process would become explosive and burdensome. An alternative to the link-based IP hopping strategy may be employed within an Ethernet network. The solution is to provide that the node linking the Internet to the Ethernet (call it the border node) use the link-based IP-hopping communication regime to communicate with nodes outside the Ethernet LAN. Within the Ethernet LAN, each TARP node would have a single IP address which would be addressed in the conventional way. Instead of comparing the {sender, receiver} IP address pairs to authenticate a packet, the intra-LAN TARP node would use one of the IP header extension fields to do so. Thus, the border node uses an algorithm shared by the intra-LAN TARP node to generate a symbol that is stored in the free field in the IP header, and the intra-LAN TARP node generates a range of symbols based on its prediction of the next expected packet to be received from that particular source IP address. The packet is rejected if it does not fall into the set of predicted symbols (for example, numerical values) or is accepted if it does. Communications from the intra-LAN TARP node to the border node are accomplished in the same manner, though the algorithm will necessarily be different for security reasons. Thus, each of the communicating nodes will generate transmit and receive tables in a similar manner to that of Figure 9; the intra-LAN

TARP nodes transmit table will be identical to the border node's receive table, and the intra-LAN TARP node's receive table will be identical to the border node's transmit table.

The algorithm used for IP address-hopping can be any desired algorithm. For example, the algorithm can be a given pseudo-random number generator that generates numbers of the range covering the allowed IP addresses with a given seed. Alternatively, the session participants can assume a certain type of algorithm and specify simply a parameter for applying the algorithm. For example the assumed algorithm could be a particular pseudo-random number generator and the session participants could simply exchange seed values.

Note that there is no permanent physical distinction between the originating and destination terminal nodes. Either device at either end point can initiate a synchronization of the pair. Note also that the authentication/synchronization-request (and acknowledgment) and hopblock-exchange may all be served by a single message so that separate message exchanges may not be required.

As another extension to the stated architecture, multiple physical paths can be used by a client, in order to provide link redundancy and further thwart attempts at denial of service and traffic monitoring. As shown in Figure 10, for example, client 1001 can establish three simultaneous sessions with each of three TARP routers provided by different ISPs 1011, 1012, 1013. As an example, the client 1001 can use three different telephone lines 1021, 1022, 1023 to connect to the ISPs, or two telephone lines and a cable modem, etc. In this scheme, transmitted packets will be sent in a random fashion among the different physical paths. This architecture provides a high degree of communications redundancy, with improved immunity from denial-of-service attacks and traffic monitoring.

2. FURTHER EXTENSIONS

The following describes various extensions to the techniques, systems, and methods described above. As described above, the security of communications occurring between computers in a computer network (such as the Internet, an Ethernet, or others) can be enhanced by using seemingly random source and

destination Internet Protocol (IP) addresses for data packets transmitted over the network. This feature prevents eavesdroppers from determining which computers in the network are communicating with each other while permitting the two communicating computers to easily recognize whether a given received data packet is legitimate or not. In one embodiment of the above-described systems, an IP header extension field is used to authenticate incoming packets on an Ethernet.

Various extensions to the previously described techniques described herein include: (1) use of hopped hardware or "MAC" addresses in broadcast type network; (2) a self-synchronization technique that permits a computer to automatically regain synchronization with a sender; (3) synchronization algorithms that allow transmitting and receiving computers to quickly re-establish synchronization in the event of lost packets or other events; and (4) a fast-packet rejection mechanism for rejecting invalid packets. Any or all of these extensions can be combined with the features described above in any of various ways.

A. Hardware Address Hopping

Internet protocol-based communications techniques on a LAN—or across any dedicated physical medium—typically embed the IP packets within lower-level packets, often referred to as "frames." As shown in FIG. 11, for example, a first Ethernet frame 1150 comprises a frame header 1101 and two embedded IP packets IP1 and IP2, while a second Ethernet frame 1160 comprises a different frame header 1104 and a single IP packet IP3. Each frame header generally includes a source hardware address 1101A and a destination hardware address 1101B; other well-known fields in frame headers are omitted from FIG. 11 for clarity. Two hardware nodes communicating over a physical communication channel insert appropriate source and destination hardware addresses to indicate which nodes on the channel or network should receive the frame.

It may be possible for a nefarious listener to acquire information about the contents of a frame and/or its communicants by examining frames on a local network rather than (or in addition to) the IP packets themselves. This is especially true in broadcast media, such as Ethernet, where it is necessary to insert into the frame

header the hardware address of the machine that generated the frame and the hardware address of the machine to which frame is being sent. All nodes on the network can potentially "see" all packets transmitted across the network. This can be a problem for secure communications, especially in cases where the communicants do not want for any third party to be able to identify who is engaging in the information exchange. One way to address this problem is to push the address-hopping scheme down to the hardware layer. In accordance with various embodiments of the invention, hardware addresses are "hopped" in a manner similar to that used to change IP addresses, such that a listener cannot determine which hardware node generated a particular message nor which node is the intended recipient.

FIG. 12A shows a system in which Media Access Control ("MAC") hardware addresses are "hopped" in order to increase security over a network such as an Ethernet. While the description refers to the exemplary case of an Ethernet environment, the inventive principles are equally applicable to other types of communications media. In the Ethernet case, the MAC address of the sender and receiver are inserted into the Ethernet frame and can be observed by anyone on the LAN who is within the broadcast range for that frame. For secure communications, it becomes desirable to generate frames with MAC addresses that are not attributable to any specific sender or receiver.

As shown in FIG. 12A, two computer nodes 1201 and 1202 communicate over a communication channel such as an Ethernet. Each node executes one or more application programs 1203 and 1218 that communicate by transmitting packets through communication software 1204 and 1217, respectively. Examples of application programs include video conferencing, e-mail, word processing programs, telephony, and the like. Communication software 1204 and 1217 can comprise, for example, an OSI layered architecture or "stack" that standardizes various services provided at different levels of functionality.

The lowest levels of communication software 1204 and 1217 communicate with hardware components 1206 and 1214 respectively, each of which can include one or more registers 1207 and 1215 that allow the hardware to be reconfigured or

controlled in accordance with various communication protocols. The hardware components (an Ethernet network interface card, for example) communicate with each other over the communication medium. Each hardware component is typically pre-assigned a fixed hardware address or MAC number that identifies the hardware component to other nodes on the network. One or more interface drivers control the operation of each card and can, for example, be configured to accept or reject packets from certain hardware addresses. As will be described in more detail below, various embodiments of the inventive principles provide for "hopping" different addresses using one or more algorithms and one or more moving windows that track a range of valid addresses to validate received packets. Packets transmitted according to one or more of the inventive principles will be generally referred to as "secure" packets or "secure communications" to differentiate them from ordinary data packets that are transmitted in the clear using ordinary, machine-correlated addresses.

One straightforward method of generating non-attributable MAC addresses is an extension of the IP hopping scheme. In this scenario, two machines on the same LAN that desire to communicate in a secure fashion exchange random-number generators and seeds, and create sequences of quasi-random MAC addresses for synchronized hopping. The implementation and synchronization issues are then similar to that of IP hopping.

This approach, however, runs the risk of using MAC addresses that are currently active on the LAN—which, in turn, could interrupt communications for those machines. Since an Ethernet MAC address is at present 48 bits in length, the chance of randomly misusing an active MAC address is actually quite small. However, if that figure is multiplied by a large number of nodes (as would be found on an extensive LAN), by a large number of frames (as might be the case with packet voice or streaming video), and by a large number of concurrent Virtual Private Networks (VPNs), then the chance that a non-secure machine's MAC address could be used in an address-hopped frame can become non-trivial. In short, any scheme that runs even a small risk of interrupting communications for other machines on the LAN is bound to receive resistance from prospective system administrators. Nevertheless, it

is technically feasible, and can be implemented without risk on a LAN on which there is a small number of machines, or if all of the machines on the LAN are engaging in MAC-hopped communications.

Synchronized MAC address hopping may incur some overhead in the course of session establishment, especially if there are multiple sessions or multiple nodes involved in the communications. A simpler method of randomizing MAC addresses is to allow each node to receive and process *every* incident frame on the network. Typically, each network interface driver will check the destination MAC address in the header of every incident frame to see if it matches that machine's MAC address; if there is no match, then the frame is discarded. In one embodiment, however, these checks can be disabled, and every incident packet is passed to the TARP stack for processing. This will be referred to as "promiscuous" mode, since every incident frame is processed. Promiscuous mode allows the sender to use completely random, unsynchronized MAC addresses, since the destination machine is guaranteed to process the frame. The decision as to whether the packet was truly intended for that machine is handled by the TARP stack, which checks the source and destination IP addresses for a match in its IP synchronization tables. If no match is found, the packet is discarded; if there is a match, the packet is unwrapped, the inner header is evaluated, and if the inner header indicates that the packet is destined for that machine then the packet is forwarded to the IP stack—otherwise it is discarded.

One disadvantage of purely-random MAC address hopping is its impact on processing overhead; that is, since every incident frame must be processed, the machine's CPU is engaged considerably more often than if the network interface driver is discriminating and rejecting packets unilaterally. A compromise approach is to select either a single fixed MAC address or a small number of MAC addresses (e.g., one for each virtual private network on an Ethernet) to use for MAC-hopped communications, regardless of the actual recipient for which the message is intended. In this mode, the network interface driver can check each incident frame against one (or a few) pre-established MAC addresses, thereby freeing the CPU from the task of physical-layer packet discrimination. This scheme does not betray any useful

information to an interloper on the LAN; in particular, every secure packet can already be identified by a unique packet type in the outer header. However, since all machines engaged in secure communications would either be using the same MAC address, or be selecting from a small pool of predetermined MAC addresses, the association between a specific machine and a specific MAC address is effectively broken.

In this scheme, the CPU will be engaged more often than it would be in non-secure communications (or in synchronized MAC address hopping), since the network interface driver cannot always unilaterally discriminate between secure packets that are destined for that machine, and secure packets from other VPNs. However, the non-secure traffic is easily eliminated at the network interface, thereby reducing the amount of processing required of the CPU. There are boundary conditions where these statements would not hold, of course—e.g., if *all* of the traffic on the LAN is secure traffic, then the CPU would be engaged to the same degree as it is in the purely-random address hopping case; alternatively, if each VPN on the LAN uses a different MAC address, then the network interface can perfectly discriminate secure frames destined for the local machine from those constituting other VPNs. These are engineering tradeoffs that might be best handled by providing administrative options for the users when installing the software and/or establishing VPNs.

Even in this scenario, however, there still remains a slight risk of selecting MAC addresses that are being used by one or more nodes on the LAN. One solution to this problem is to formally assign one address or a range of addresses for use in MAC-hopped communications. This is typically done via an assigned numbers registration authority; e.g., in the case of Ethernet, MAC address ranges are assigned to vendors by the Institute of Electrical and Electronics Engineers (IEEE). A formally-assigned range of addresses would ensure that secure frames do not conflict with any properly-configured and properly-functioning machines on the LAN.

Reference will now be made to FIGS. 12A and 12B in order to describe the many combinations and features that follow the inventive principles. As explained

above, two computer nodes 1201 and 1202 are assumed to be communicating over a network or communication medium such as an Ethernet. A communication protocol in each node (1204 and 1217, respectively) contains a modified element 1205 and 1216 that performs certain functions that deviate from the standard communication protocols. In particular, computer node 1201 implements a first "hop" algorithm 1208X that selects seemingly random source and destination IP addresses (and, in one embodiment, seemingly random IP header discriminator fields) in order to transmit each packet to the other computer node. For example, node 1201 maintains a transmit table 1208 containing triplets of source (S), destination (D), and discriminator fields (DS) that are inserted into outgoing IP packet headers. The table is generated through the use of an appropriate algorithm (e.g., a random number generator that is seeded with an appropriate seed) that is known to the recipient node 1202. As each new IP packet is formed, the next sequential entry out of the sender's transmit table 1208 is used to populate the IP source, IP destination, and IP header extension field (e.g., discriminator field). It will be appreciated that the transmit table need not be created in advance but could instead be created on-the-fly by executing the algorithm when each packet is formed.

At the receiving node 1202, the same IP hop algorithm 1222X is maintained and used to generate a receive table 1222 that lists valid triplets of source IP address, destination IP address, and discriminator field. This is shown by virtue of the first five entries of transmit table 1208 matching the second five entries of receive table 1222. (The tables may be slightly offset at any particular time due to lost packets, misordered packets, or transmission delays). Additionally, node 1202 maintains a receive window W3 that represents a list of valid IP source, IP destination, and discriminator fields that will be accepted when received as part of an incoming IP packet. As packets are received, window W3 slides down the list of valid entries, such that the possible valid entries change over time. Two packets that arrive out of order but are nevertheless matched to entries within window W3 will be accepted; those falling outside of window W3 will be rejected as invalid. The length of window W3 can be adjusted as necessary to reflect network delays or other factors.

Node 1202 maintains a similar transmit table 1221 for creating IP packets and frames destined for node 1201 using a potentially different hopping algorithm 1221X, and node 1201 maintains a matching receive table 1209 using the same algorithm 1209X. As node 1202 transmits packets to node 1201 using seemingly random IP source, IP destination, and/or discriminator fields, node 1201 matches the incoming packet values to those falling within window W1 maintained in its receive table. In effect, transmit table 1208 of node 1201 is synchronized (i.e., entries are selected in the same order) to receive table 1222 of receiving node 1202. Similarly, transmit table 1221 of node 1202 is synchronized to receive table 1209 of node 1201. It will be appreciated that although a common algorithm is shown for the source, destination and discriminator fields in FIG. 12A (using, e.g., a different seed for each of the three fields), an entirely different algorithm could in fact be used to establish values for each of these fields. It will also be appreciated that one or two of the fields can be "hopped" rather than all three as illustrated.

In accordance with another aspect of the invention, hardware or "MAC" addresses are hopped instead of or in addition to IP addresses and/or the discriminator field in order to improve security in a local area or broadcast-type network. To that end, node 1201 further maintains a transmit table 1210 using a transmit algorithm 1210X to generate source and destination hardware addresses that are inserted into frame headers (e.g., fields 1101A and 1101B in FIG. 11) that are synchronized to a corresponding receive table 1224 at node 1202. Similarly, node 1202 maintains a different transmit table 1223 containing source and destination hardware addresses that is synchronized with a corresponding receive table 1211 at node 1201. In this manner, outgoing hardware frames appear to be originating from and going to completely random nodes on the network, even though each recipient can determine whether a given packet is intended for it or not. It will be appreciated that the hardware hopping feature can be implemented at a different level in the communications protocol than the IP hopping feature (e.g., in a card driver or in a hardware card itself to improve performance).

FIG. 12B shows three different embodiments or modes that can be employed using the aforementioned principles. In a first mode referred to as "promiscuous" mode, a common hardware address (e.g., a fixed address for source and another for destination) or else a completely random hardware address is used by all nodes on the network, such that a particular packet cannot be attributed to any one node. Each node must initially accept all packets containing the common (or random) hardware address and inspect the IP addresses or discriminator field to determine whether the packet is intended for that node. In this regard, either the IP addresses or the discriminator field or both can be varied in accordance with an algorithm as described above. As explained previously, this may increase each node's overhead since additional processing is involved to determine whether a given packet has valid source and destination hardware addresses.

In a second mode referred to as "promiscuous per VPN" mode, a small set of fixed hardware addresses are used, with a fixed source/destination hardware address used for all nodes communicating over a virtual private network. For example, if there are six nodes on an Ethernet, and the network is to be split up into two private virtual networks such that nodes on one VPN can communicate with only the other two nodes on its own VPN, then two sets of hardware addresses could be used: one set for the first VPN and a second set for the second VPN. This would reduce the amount of overhead involved in checking for valid frames since only packets arriving from the designated VPN would need to be checked. IP addresses and one or more discriminator fields could still be hopped as before for secure communication within the VPN. Of course, this solution compromises the anonymity of the VPNs (i.e., an outsider can easily tell what traffic belongs in which VPN, though he cannot correlate it to a specific machine/person). It also requires the use of a discriminator field to mitigate the vulnerability to certain types of DoS attacks. (For example, without the discriminator field, an attacker on the LAN could stream frames containing the MAC addresses being used by the VPN; rejecting those frames could lead to excessive processing overhead. The discriminator field would provide a low-overhead means of rejecting the false packets.)

In a third mode referred to as "hardware hopping" mode, hardware addresses are varied as illustrated in FIG. 12A, such that hardware source and destination addresses are changed constantly in order to provide non-attributable addressing. Variations on these embodiments are of course possible, and the invention is not intended to be limited in any respect by these illustrative examples.

B. Extending the Address Space

Address hopping provides security and privacy. However, the level of protection is limited by the number of addresses in the blocks being hopped. A hopblock denotes a field or fields modulated on a packet-wise basis for the purpose of providing a VPN. For instance, if two nodes communicate with IP address hopping using hopblocks of 4 addresses (2 bits) each, there would be 16 possible address-pair combinations. A window of size 16 would result in most address pairs being accepted as valid most of the time. This limitation can be overcome by using a discriminator field in addition to or instead of the hopped address fields. The discriminator field would be hopped in exactly the same fashion as the address fields and it would be used to determine whether a packet should be processed by a receiver.

Suppose that two clients, each using four-bit hopblocks, would like the same level of protection afforded to clients communicating via IP hopping between two A blocks (24 address bits eligible for hopping). A discriminator field of 20 bits, used in conjunction with the 4 address bits eligible for hopping in the IP address field, provides this level of protection. A 24-bit discriminator field would provide a similar level of protection if the address fields were not hopped or ignored. Using a discriminator field offers the following advantages: (1) an arbitrarily high level of protection can be provided, and (2) address hopping is unnecessary to provide protection. This may be important in environments where address hopping would cause routing problems.

C. Synchronization Techniques

It is generally assumed that once a sending node and receiving node have exchanged algorithms and seeds (or similar information sufficient to generate quasi-random source and destination tables), subsequent communication between the two nodes will proceed smoothly. Realistically, however, two nodes may lose synchronization due to network delays or outages, or other problems. Consequently, it is desirable to provide means for re-establishing synchronization between nodes in a network that have lost synchronization.

One possible technique is to require that each node provide an acknowledgment upon successful receipt of each packet and, if no acknowledgment is received within a certain period of time, to re-send the unacknowledged packet. This approach, however, drives up overhead costs and may be prohibitive in high-throughput environments such as streaming video or audio, for example.

A different approach is to employ an automatic synchronizing technique that will be referred to herein as "self-synchronization." In this approach, synchronization information is embedded into each packet, thereby enabling the receiver to re-synchronize itself upon receipt of a single packet if it determines that is has lost synchronization with the sender. (If communications are already in progress, and the receiver determines that it is still in sync with the sender, then there is no need to re-synchronize.) A receiver could detect that it was out of synchronization by, for example, employing a "dead-man" timer that expires after a certain period of time, wherein the timer is reset with each valid packet. A time stamp could be hashed into the public sync field (see below) to preclude packet-retry attacks.

In one embodiment, a "sync field" is added to the header of each packet sent out by the sender. This sync field could appear in the clear or as part of an encrypted portion of the packet. Assuming that a sender and receiver have selected a random-number generator (RNG) and seed value, this combination of RNG and seed can be used to generate a random-number sequence (RNS). The RNS is then used to generate a sequence of source/destination IP pairs (and, if desired, discriminator fields and hardware source and destination addresses), as described above. It is not necessary,

however, to generate the entire sequence (or the first N-1 values) in order to generate the Nth random number in the sequence; if the sequence index N is known, the random value corresponding to that index can be directly generated (see below). Different RNGs (and seeds) with different fundamental periods could be used to generate the source and destination IP sequences, but the basic concepts would still apply. For the sake of simplicity, the following discussion will assume that IP source and destination address pairs (only) are hopped using a single RNG sequencing mechanism.

In accordance with a "self-synchronization" feature, a sync field in each packet header provides an index (i.e., a sequence number) into the RNS that is being used to generate IP pairs. Plugging this index into the RNG that is being used to generate the RNS yields a specific random number value, which in turn yields a specific IP pair. That is, an IP pair can be generated directly from knowledge of the RNG, seed, and index number; it is not necessary, in this scheme, to generate the entire sequence of random numbers that precede the sequence value associated with the index number provided.

Since the communicants have presumably previously exchanged RNGs and seeds, the only new information that must be provided in order to generate an IP pair is the sequence number. If this number is provided by the sender in the packet header, then the receiver need only plug this number into the RNG in order to generate an IP pair – and thus verify that the IP pair appearing in the header of the packet is valid. In this scheme, if the sender and receiver lose synchronization, the receiver can immediately re-synchronize upon receipt of a single packet by simply comparing the IP pair in the packet header to the IP pair generated from the index number. Thus, synchronized communications can be resumed upon receipt of a single packet, making this scheme ideal for multicast communications. Taken to the extreme, it could obviate the need for synchronization tables entirely; that is, the sender and receiver could simply rely on the index number in the sync field to validate the IP pair on each packet, and thereby eliminate the tables entirely.

The aforementioned scheme may have some inherent security issues associated with it — namely, the placement of the sync field. If the field is placed in the outer header, then an interloper could observe the values of the field and their relationship to the IP stream. This could potentially compromise the algorithm that is being used to generate the IP-address sequence, which would compromise the security of the communications. If, however, the value is placed in the inner header, then the sender must decrypt the inner header before it can extract the sync value and validate the IP pair; this opens up the receiver to certain types of denial-of-service (DoS) attacks, such as packet replay. That is, if the receiver must decrypt a packet before it can validate the IP pair, then it could potentially be forced to expend a significant amount of processing on decryption if an attacker simply retransmits previously valid packets. Other attack methodologies are possible in this scenario.

A possible compromise between algorithm security and processing speed is to split up the sync value between an inner (encrypted) and outer (unencrypted) header. That is, if the sync value is sufficiently long, it could potentially be split into a rapidly-changing part that can be viewed in the clear, and a fixed (or very slowly changing) part that must be protected. The part that can be viewed in the clear will be called the "public sync" portion and the part that must be protected will be called the "private sync" portion.

Both the public sync and private sync portions are needed to generate the complete sync value. The private portion, however, can be selected such that it is fixed or will change only occasionally. Thus, the private sync value can be stored by the recipient, thereby obviating the need to decrypt the header in order to retrieve it. If the sender and receiver have previously agreed upon the frequency with which the private part of the sync will change, then the receiver can selectively decrypt a single header in order to extract the new private sync if the communications gap that has led to lost synchronization has exceeded the lifetime of the previous private sync. This should not represent a burdensome amount of decryption, and thus should not open up the receiver to denial-of-service attack simply based on the need to occasionally decrypt a single header.

One implementation of this is to use a hashing function with a one-to-one mapping to generate the private and public sync portions from the sync value. This implementation is shown in FIG. 13, where (for example) a first ISP 1302 is the sender and a second ISP 1303 is the receiver. (Other alternatives are possible from FIG. 13.) A transmitted packet comprises a public or "outer" header 1305 that is not encrypted, and a private or "inner" header 1306 that is encrypted using for example a link key. Outer header 1305 includes a public sync portion while inner header 1306 contains the private sync portion. A receiving node decrypts the inner header using a decryption function 1307 in order to extract the private sync portion. This step is necessary only if the lifetime of the currently buffered private sync has expired. (If the currently-buffered private sync is still valid, then it is simply extracted from memory and "added" (which could be an inverse hash) to the public sync, as shown in step 1308.) The public and decrypted private sync portions are combined in function 1308 in order to generate the combined sync 1309. The combined sync (1309) is then fed into the RNG (1310) and compared to the IP address pair (1311) to validate or reject the packet.

An important consideration in this architecture is the concept of "future" and "past" where the public sync values are concerned. Though the sync values, themselves, should be random to prevent spoofing attacks, it may be important that the receiver be able to quickly identify a sync value that has already been sent — even if the packet containing that sync value was never actually received by the receiver. One solution is to hash a time stamp or sequence number into the public sync portion, which could be quickly extracted, checked, and discarded, thereby validating the public sync portion itself.

In one embodiment, packets can be checked by comparing the source/destination IP pair generated by the sync field with the pair appearing in the packet header. If (1) they match, (2) the time stamp is valid, and (3) the dead-man timer has expired, then re-synchronization occurs; otherwise, the packet is rejected. If enough processing power is available, the dead-man timer and synchronization tables

can be avoided altogether, and the receiver would simply resynchronize (e.g., validate) on every packet.

The foregoing scheme may require large-integer (e.g., 160-bit) math, which may affect its implementation. Without such large-integer registers, processing throughput would be affected, thus potentially affecting security from a denial-of-service standpoint. Nevertheless, as large-integer math processing features become more prevalent, the costs of implementing such a feature will be reduced.

D. Other Synchronization Schemes

As explained above, if W or more consecutive packets are lost between a transmitter and receiver in a VPN (where W is the window size), the receiver's window will not have been updated and the transmitter will be transmitting packets not in the receiver's window. The sender and receiver will not recover synchronization until perhaps the random pairs in the window are repeated by chance. Therefore, there is a need to keep a transmitter and receiver in synchronization whenever possible and to re-establish synchronization whenever it is lost.

A "checkpoint" scheme can be used to regain synchronization between a sender and a receiver that have fallen out of synchronization. In this scheme, a checkpoint message comprising a random IP address pair is used for communicating synchronization information. In one embodiment, two messages are used to communicate synchronization information between a sender and a recipient:

1. SYNC_REQ is a message used by the sender to indicate that it wants to synchronize; and
2. SYNC_ACK is a message used by the receiver to inform the transmitter that it has been synchronized.

According to one variation of this approach, both the transmitter and receiver maintain three checkpoints (see FIG. 14):

1. In the transmitter, ckpt_o ("checkpoint old") is the IP pair that was used to re-send the last SYNC_REQ packet to the receiver. In the receiver, ckpt_o ("checkpoint old") is the IP pair that receives repeated SYNC_REQ packets from the transmitter.

2. In the transmitter, ckpt_n ("checkpoint new") is the IP pair that will be used to send the next SYNC_REQ packet to the receiver. In the receiver, ckpt_n ("checkpoint new") is the IP pair that receives a new SYNC_REQ packet from the transmitter and which causes the receiver's window to be re-aligned, ckpt_o set to ckpt_n, a new ckpt_n to be generated and a new ckpt_r to be generated.
3. In the transmitter, ckpt_r is the IP pair that will be used to send the next SYNC_ACK packet to the receiver. In the receiver, ckpt_r is the IP pair that receives a new SYNC_ACK packet from the transmitter and which causes a new ckpt_n to be generated. Since SYNC_ACK is transmitted from the receiver ISP to the sender ISP, the transmitter ckpt_r refers to the ckpt_r of the receiver and the receiver ckpt_r refers to the ckpt_r of the transmitter (see FIG. 14).

When a transmitter initiates synchronization, the IP pair it will use to transmit the next data packet is set to a predetermined value and when a receiver first receives a SYNC_REQ, the receiver window is updated to be centered on the transmitter's next IP pair. This is the primary mechanism for checkpoint synchronization.

Synchronization can be initiated by a packet counter (e.g., after every N packets transmitted, initiate a synchronization) or by a timer (every S seconds, initiate a synchronization) or a combination of both. See FIG. 15. From the transmitter's perspective, this technique operates as follows: (1) Each transmitter periodically transmits a "sync request" message to the receiver to make sure that it is in sync. (2) If the receiver is still in sync, it sends back a "sync ack" message. (If this works, no further action is necessary). (3) If no "sync ack" has been received within a period of time, the transmitter retransmits the sync request again. If the transmitter reaches the next checkpoint without receiving a "sync ack" response, then synchronization is broken, and the transmitter should stop transmitting. The transmitter will continue to send sync_reqs until it receives a sync_ack , at which point transmission is reestablished.

From the receiver's perspective, the scheme operates as follows: (1) when it receives a "sync request" request from the transmitter, it advances its window to the next checkpoint position (even skipping pairs if necessary), and sends a "sync ack" message to the transmitter. If sync was never lost, then the "jump ahead" really just advances to the next available pair of addresses in the table (i.e., normal advancement).

If an interloper intercepts the "sync request" messages and tries to interfere with communication by sending new ones, it will be ignored if the synchronization has been established or it it will actually help to re-establish synchronization.

A window is realigned whenever a re-synchronization occurs. This realignment entails updating the receiver's window to straddle the address pairs used by the packet transmitted immediately after the transmission of the SYNC_REQ packet. Normally, the transmitter and receiver are in synchronization with one another. However, when network events occur, the receiver's window may have to be advanced by many steps during resynchronization. In this case, it is desirable to move the window ahead without having to step through the intervening random numbers sequentially. (This feature is also desirable for the auto-sync approach discussed above).

E. Random Number Generator with a Jump-Ahead capability

An attractive method for generating randomly hopped addresses is to use identical random number generators in the transmitter and receiver and advance them as packets are transmitted and received. There are many random number generation algorithms that could be used. Each one has strengths and weaknesses for address hopping applications.

Linear congruential random number generators (LCRs) are fast, simple and well characterized random number generators that can be made to jump ahead n steps efficiently. An LCR generates random numbers $X_1, X_2, X_3 \ldots X_k$ starting with seed X_0 using a recurrence

$$X_i=(a\,X_{i-1} + b) \bmod c, \qquad (1)$$

where a, b and c define a particular LCR. Another expression for X_i,

$$X_i=((a^i(X_0+b)-b)/(a-1)) \bmod c \quad (2)$$

enables the jump-ahead capability. The factor a^i can grow very large even for modest i if left unfettered. Therefore some special properties of the modulo operation can be used to control the size and processing time required to compute (2). (2) can be rewritten as:

$$X_i=(a^i (X_0(a-1)+b)-b)/(a-1) \bmod c. \quad (3)$$

It can be shown that:

$$(a^i(X_0(a-1)+b)-b)/(a-1) \bmod c =$$

$$((a^i \bmod((a-1)c)(X_0(a-1)+b) -b) /(a-1)) \bmod c \quad (4).$$

$(X_0(a-1)+b)$ can be stored as $(X_0(a-1)+b) \bmod c$, b as b mod c and compute $a^i \bmod((a-1)c)$ (this requires O(log(i)) steps).

A practical implementation of this algorithm would jump a fixed distance, n, between synchronizations; this is tantamount to synchronizing every *n* packets. The window would commence *n* IP pairs from the start of the previous window. Using X_j^w, the random number at the jth checkpoint, as X_0 and *n* as *i*, a node can store $a^n \bmod((a-1)c)$ once per LCR and set

$$X_{j+1}^w=X_{n(j+1)}=((a^n \bmod((a-1)c) (X_j^w (a-1)+b)-b)/(a-1))\bmod c, \quad (5)$$

to generate the random number for the $j+1^{th}$ synchronization. Using this construction, a node could jump ahead an arbitrary (but fixed) distance between synchronizations in a constant amount of time (independent of n).

Pseudo-random number generators, in general, and LCRs, in particular, will eventually repeat their cycles. This repetition may present vulnerability in the IP hopping scheme. An adversary would simply have to wait for a repeat to predict future sequences. One way of coping with this vulnerability is to create a random number generator with a known long cycle. A random sequence can be replaced by a new random number generator before it repeats. LCRs can be constructed with known long cycles. This is not currently true of many random number generators.

Random number generators can be cryptographically insecure. An adversary can derive the RNG parameters by examining the output or part of the output. This is true of LCGs. This vulnerability can be mitigated by incorporating an encryptor,

designed to scramble the output as part of the random number generator. The random number generator prevents an adversary from mounting an attack—e.g., a known plaintext attack—against the encryptor.

F. Random Number Generator Example

Consider a RNG where a=31,b=4 and c=15. For this case equation (1) becomes:

$X_i=(31\ X_{i-1}+4) \bmod 15$. (6)

If one sets $X_0=1$, equation (6) will produce the sequence 1, 5, 9, 13, 2, 6, 10, 14, 3, 7, 11, 0, 4, 8, 12. This sequence will repeat indefinitely. For a jump ahead of 3 numbers in this sequence $a^n= 31^3=29791$, $c*(a-1)=15*30=450$ and $a^n \bmod((a-1)c) = 31^3 \bmod(15*30)=29791 \bmod(450)=91$. Equation (5) becomes:

$((91\ (X_i30+4)-4)/30) \bmod 15$ (7).

Table 1 shows the jump ahead calculations from (7) . The calculations start at 5 and jump ahead 3.

TABLE 1

I	X_i	(X_i30+4)	$91\ (X_i30+4)-4$	$((91\ (X_i30+4)-4)/30$	X_{i+3}
1	5	154	14010	467	2
4	2	64	5820	194	14
7	14	424	38580	1286	11
10	11	334	30390	1013	8
13	8	244	22200	740	5

G. Fast Packet Filter

Address hopping VPNs must rapidly determine whether a packet has a valid header and thus requires further processing, or has an invalid header (a hostile packet) and should be immediately rejected. Such rapid determinations will be referred to as "fast packet filtering." This capability protects the VPN from attacks by an adversary who streams hostile packets at the receiver at a high rate of speed in the hope of saturating the receiver's processor (a so-called "denial of service" attack). Fast packet

filtering is an important feature for implementing VPNs on shared media such as Ethernet.

Assuming that all participants in a VPN share an unassigned "A" block of addresses, one possibility is to use an experimental "A" block that will never be assigned to any machine that is not address hopping on the shared medium. "A" blocks have a 24 bits of address that can be hopped as opposed to the 8 bits in "C" blocks. In this case a hopblock will be the "A" block. The use of the experimental "A" block is a likely option on an Ethernet because:

1. The addresses have no validity outside of the Ethernet and will not be routed out to a valid outside destination by a gateway.
2. There are 2^{24} (~16 million) addresses that can be hopped within each "A" block. This yields >280 trillion possible address pairs making it very unlikely that an adversary would guess a valid address. It also provides acceptably low probability of collision between separate VPNs (all VPNs on a shared medium independently generate random address pairs from the same "A" block).
3. The packets will not be received by someone on the Ethernet who is not on a VPN (unless the machine is in promiscuous mode) minimizing impact on non-VPN computers.

The Ethernet example will be used to describe one implementation of fast packet filtering. The ideal algorithm would quickly examine a packet header, determine whether the packet is hostile, and reject any hostile packets or determine which active IP pair the packet header matches. The problem is a classical associative memory problem. A variety of techniques have been developed to solve this problem (hashing, B–trees etc). Each of these approaches has its strengths and weaknesses. For instance, hash tables can be made to operate quite fast in a statistical sense, but can occasionally degenerate into a much slower algorithm. This slowness can persist for a period of time. Since there is a need to discard hostile packets quickly at all times, hashing would be unacceptable.

H. Presence Vector Algorithm

A presence vector is a bit vector of length 2^n that can be indexed by n-bit numbers (each ranging from 0 to 2^n-1). One can indicate the presence of k n-bit numbers (not necessarily unique), by setting the bits in the presence vector indexed by each number to 1. Otherwise, the bits in the presence vector are 0. An n-bit number, x, is one of the k numbers if and only if the xth bit of the presence vector is 1. A fast packet filter can be implemented by indexing the presence vector and looking for a 1, which will be referred to as the "test."

For example, suppose one wanted to represent the number 135 using a presence vector. The 135th bit of the vector would be set. Consequently, one could very quickly determine whether an address of 135 was valid by checking only one bit: the 135th bit. The presence vectors could be created in advance corresponding to the table entries for the IP addresses. In effect, the incoming addresses can be used as indices into a long vector, making comparisons very fast. As each RNG generates a new address, the presence vector is updated to reflect the information. As the window moves, the presence vector is updated to zero out addresses that are no longer valid.

There is a trade-off between efficiency of the test and the amount of memory required for storing the presence vector(s). For instance, if one were to use the 48 bits of hopping addresses as an index, the presence vector would have to be 35 terabytes. Clearly, this is too large for practical purposes. Instead, the 48 bits can be divided into several smaller fields. For instance, one could subdivide the 48 bits into four 12-bit fields (see FIG. 16). This reduces the storage requirement to 2048 bytes at the expense of occasionally having to process a hostile packet. In effect, instead of one long presence vector, the decomposed address portions must match all four shorter presence vectors before further processing is allowed. (If the first part of the address portion doesn't match the first presence vector, there is no need to check the remaining three presence vectors).

A presence vector will have a 1 in the yth bit if and only if one or more addresses with a corresponding field of y are active. An address is active only if each presence vector indexed by the appropriate sub-field of the address is 1.

Consider a window of 32 active addresses and 3 checkpoints. A hostile packet will be rejected by the indexing of one presence vector more than 99% of the time. A hostile packet will be rejected by the indexing of all 4 presence vectors more than 99.9999995% of the time. On average, hostile packets will be rejected in less than 1.02 presence vector index operations.

The small percentage of hostile packets that pass the fast packet filter will be rejected when matching pairs are not found in the active window or are active checkpoints. Hostile packets that serendipitously match a header will be rejected when the VPN software attempts to decrypt the header. However, these cases will be extremely rare. There are many other ways this method can be configured to arbitrate the space/speed tradeoffs.

I. Further Synchronization Enhancements

A slightly modified form of the synchronization techniques described above can be employed. The basic principles of the previously described checkpoint synchronization scheme remain unchanged. The actions resulting from the reception of the checkpoints are, however, slightly different. In this variation, the receiver will maintain between OoO ("Out of Order") and 2×WINDOW_SIZE+OoO active addresses ($1 \leq OoO \leq WINDOW\_SIZE$ and $WINDOW\_SIZE \geq 1$). OoO and WINDOW_SIZE are engineerable parameters, where OoO is the minimum number of addresses needed to accommodate lost packets due to events in the network or out of order arrivals and WINDOW_SIZE is the number of packets transmitted before a SYNC_REQ is issued. FIG. 17 depicts a storage array for a receiver's active addresses.

The receiver starts with the first 2×WINDOW_SIZE addresses loaded and active (ready to receive data). As packets are received, the corresponding entries are marked as "used" and are no longer eligible to receive packets. The transmitter maintains a packet counter, initially set to 0, containing the number of data packets transmitted since the last *initial* transmission of a SYNC_REQ for which SYNC_ACK has been received. When the transmitter packet counter equals WINDOW_SIZE, the transmitter generates a SYNC_REQ and does its initial

transmission. When the receiver receives a SYNC_REQ corresponding to its current CKPT_N, it generates the next WINDOW_SIZE addresses and starts loading them in order starting at the first location after the last active address wrapping around to the beginning of the array after the end of the array has been reached. The receiver's array might look like FIG. 18 when a SYNC_REQ has been received. In this case a couple of packets have been either lost or will be received out of order when the SYNC_REQ is received.

FIG. 19 shows the receiver's array after the new addresses have been generated. If the transmitter does not receive a SYNC_ACK, it will re-issue the SYNC_REQ at regular intervals. When the transmitter receives a SYNC_ACK, the packet counter is decremented by WINDOW_SIZE. If the packet counter reaches 2×WINDOW_SIZE – OoO then the transmitter ceases sending data packets until the appropriate SYNC_ACK is finally received. The transmitter then resumes sending data packets. Future behavior is essentially a repetition of this initial cycle. The advantages of this approach are:

1. There is no need for an efficient jump ahead in the random number generator,
2. No packet is ever transmitted that does not have a corresponding entry in the receiver side
3. No timer based re-synchronization is necessary. This is a consequence of 2.
4. The receiver will always have the ability to accept data messages transmitted within OoO messages of the most recently transmitted message.

J. Distributed Transmission Path Variant

Another embodiment incorporating various inventive principles is shown in FIG. 20. In this embodiment, a message transmission system includes a first computer 2001 in communication with a second computer 2002 through a network 2011 of intermediary computers. In one variant of this embodiment, the network includes two edge routers 2003 and 2004 each of which is linked to a plurality of Internet Service Providers (ISPs) 2005 through 2010. Each ISP is coupled to a plurality of other ISPs in an arrangement as shown in FIG. 20, which is a representative configuration only and is not intended to be limiting. Each connection

between ISPs is labeled in FIG. 20 to indicate a specific physical transmission path (e.g., AD is a physical path that links ISP A (element 2005) to ISP D (element 2008)). Packets arriving at each edge router are selectively transmitted to one of the ISPs to which the router is attached on the basis of a randomly or quasi-randomly selected basis.

As shown in FIG. 21, computer 2001 or edge router 2003 incorporates a plurality of link transmission tables 2100 that identify, for each potential transmission path through the network, valid sets of IP addresses that can be used to transmit the packet. For example, AD table 2101 contains a plurality of IP source/destination pairs that are randomly or quasi-randomly generated. When a packet is to be transmitted from first computer 2001 to second computer 2002, one of the link tables is randomly (or quasi-randomly) selected, and the next valid source/destination address pair from that table is used to transmit the packet through the network. If path AD is randomly selected, for example, the next source/destination IP address pair (which is pre-determined to transmit between ISP A (element 2005) and ISP B (element 2008)) is used to transmit the packet. If one of the transmission paths becomes degraded or inoperative, that link table can be set to a "down" condition as shown in table 2105, thus preventing addresses from being selected from that table. Other transmission paths would be unaffected by this broken link.

3. CONTINUATION-IN-PART IMPROVEMENTS

The following describes various improvements and features that can be applied to the embodiments described above. The improvements include: (1) a load balancer that distributes packets across different transmission paths according to transmission path quality; (2) a DNS proxy server that transparently creates a virtual private network in response to a domain name inquiry; (3) a large-to-small link bandwidth management feature that prevents denial-of-service attacks at system chokepoints; (4) a traffic limiter that regulates incoming packets by limiting the rate at which a transmitter can be synchronized with a receiver; and (5) a signaling synchronizer that allows a large number of nodes to communicate with a central node

by partitioning the communication function between two separate entities. Each is discussed separately below.

A. Load Balancer

Various embodiments described above include a system in which a transmitting node and a receiving node are coupled through a plurality of transmission paths, and wherein successive packets are distributed quasi-randomly over the plurality of paths. See, for example, FIGS. 20 and 21 and accompanying description. The improvement extends this basic concept to encompass distributing packets across different paths in such a manner that the loads on the paths are generally balanced according to transmission link quality.

In one embodiment, a system includes a transmitting node and a receiving node that are linked via a plurality of transmission paths having potentially varying transmission quality. Successive packets are transmitted over the paths based on a weight value distribution function for each path. The rate that packets will be transmitted over a given path can be different for each path. The relative "health" of each transmission path is monitored in order to identify paths that have become degraded. In one embodiment, the health of each path is monitored in the transmitter by comparing the number of packets transmitted to the number of packet acknowledgements received. Each transmission path may comprise a physically separate path (e.g., via dial-up phone line, computer network, router, bridge, or the like), or may comprise logically separate paths contained within a broadband communication medium (e.g., separate channels in an FDM, TDM, CDMA, or other type of modulated or unmodulated transmission link).

When the transmission quality of a path falls below a predetermined threshold and there are other paths that can transmit packets, the transmitter changes the weight value used for that path, making it less likely that a given packet will be transmitted over that path. The weight will preferably be set no lower than a minimum value that keeps nominal traffic on the path. The weights of the other available paths are altered to compensate for the change in the affected path. When the quality of a path degrades to where the transmitter is turned off by the synchronization function (i.e., no packets

are arriving at the destination), the weight is set to zero. If all transmitters are turned off, no packets are sent.

Conventional TCP/IP protocols include a "throttling" feature that reduces the transmission rate of packets when it is determined that delays or errors are occurring in transmission. In this respect, timers are sometimes used to determine whether packets have been received. These conventional techniques for limiting transmission of packets, however, do not involve multiple transmission paths between two nodes wherein transmission across a particular path relative to the others is changed based on link quality.

According to certain embodiments, in order to damp oscillations that might otherwise occur if weight distributions are changed drastically (e.g., according to a step function), a linear or an exponential decay formula can be applied to gradually decrease the weight value over time that a degrading path will be used. Similarly, if the health of a degraded path improves, the weight value for that path is gradually increased.

Transmission link health can be evaluated by comparing the number of packets that are acknowledged within the transmission window (see embodiments discussed above) to the number of packets transmitted within that window and by the state of the transmitter (i.e., on or off). In other words, rather than accumulating general transmission statistics over time for a path, one specific implementation uses the "windowing" concepts described above to evaluate transmission path health.

The same scheme can be used to shift virtual circuit paths from an "unhealthy" path to a "healthy" one, and to select a path for a new virtual circuit.

FIG. 22A shows a flowchart for adjusting weight values associated with a plurality of transmission links. It is assumed that software executing in one or more computer nodes executes the steps shown in FIG. 22A. It is also assumed that the software can be stored on a computer-readable medium such as a magnetic or optical disk for execution by a computer.

Beginning in step 2201, the transmission quality of a given transmission path is measured. As described above, this measurement can be based on a comparison

between the number of packets transmitted over a particular link to the number of packet acknowledgements received over the link (e.g., per unit time, or in absolute terms). Alternatively, the quality can be evaluated by comparing the number of packets that are acknowledged within the transmission window to the number of packets that were transmitted within that window. In yet another variation, the number of missed synchronization messages can be used to indicate link quality. Many other variations are of course possible.

In step 2202, a check is made to determine whether more than one transmitter (e.g., transmission path) is turned on. If not, the process is terminated and resumes at step 2201.

In step 2203, the link quality is compared to a given threshold (e.g., 50%, or any arbitrary number). If the quality falls below the threshold, then in step 2207 a check is made to determine whether the weight is above a minimum level (e.g., 1%). If not, then in step 2209 the weight is set to the minimum level and processing resumes at step 2201. If the weight is above the minimum level, then in step 2208 the weight is gradually decreased for the path, then in step 2206 the weights for the remaining paths are adjusted accordingly to compensate (e.g., they are increased).

If in step 2203 the quality of the path was greater than or equal to the threshold, then in step 2204 a check is made to determine whether the weight is less than a steady-state value for that path. If so, then in step 2205 the weight is increased toward the steady-state value, and in step 2206 the weights for the remaining paths are adjusted accordingly to compensate (e.g., they are decreased). If in step 2204 the weight is not less than the steady-state value, then processing resumes at step 2201 without adjusting the weights.

The weights can be adjusted incrementally according to various functions, preferably by changing the value gradually. In one embodiment, a linearly decreasing function is used to adjust the weights; according to another embodiment, an exponential decay function is used. Gradually changing the weights helps to damp oscillators that might otherwise occur if the probabilities were abruptly.

Although not explicitly shown in FIG. 22A the process can be performed only periodically (e.g., according to a time schedule), or it can be continuously run, such as in a background mode of operation. In one embodiment, the combined weights of all potential paths should add up to unity (e.g., when the weighting for one path is decreased, the corresponding weights that the other paths will be selected will increase).

Adjustments to weight values for other paths can be prorated. For example, a decrease of 10% in weight value for one path could result in an evenly distributed increase in the weights for the remaining paths. Alternatively, weightings could be adjusted according to a weighted formula as desired (e.g., favoring healthy paths over less healthy paths). In yet another variation, the difference in weight value can be amortized over the remaining links in a manner that is proportional to their traffic weighting.

FIG. 22B shows steps that can be executed to shut down transmission links where a transmitter turns off. In step 2210, a transmitter shut-down event occurs. In step 2211, a test is made to determine whether at least one transmitter is still turned on. If not, then in step 2215 all packets are dropped until a transmitter turns on. If in step 2211 at least one transmitter is turned on, then in step 2212 the weight for the path is set to zero, and the weights for the remaining paths are adjusted accordingly.

FIG. 23 shows a computer node 2301 employing various principles of the above-described embodiments. It is assumed that two computer nodes of the type shown in FIG. 23 communicate over a plurality of separate physical transmission paths. As shown in FIG. 23, four transmission paths X1 through X4 are defined for communicating between the two nodes. Each node includes a packet transmitter 2302 that operates in accordance with a transmit table 2308 as described above. (The packet transmitter could also operate without using the IP-hopping features described above, but the following description assumes that some form of hopping is employed in conjunction with the path selection mechanism.). The computer node also includes a packet receiver 2303 that operates in accordance with a receive table 2309, including a moving window W that moves as valid packets are received. Invalid

packets having source and destination addresses that do not fall within window W are rejected.

As each packet is readied for transmission, source and destination IP addresses (or other discriminator values) are selected from transmit table 2308 according to any of the various algorithms described above, and packets containing these source/destination address pairs, which correspond to the node to which the four transmission paths are linked, are generated to a transmission path switch 2307. Switch 2307, which can comprise a software function, selects from one of the available transmission paths according to a weight distribution table 2306. For example, if the weight for path X1 is 0.2, then every fifth packet will be transmitted on path X1. A similar regime holds true for the other paths as shown. Initially, each link's weight value can be set such that it is proportional to its bandwidth, which will be referred to as its "steady-state" value.

Packet receiver 2303 generates an output to a link quality measurement function 2304 that operates as described above to determine the quality of each transmission path. (The input to packet receiver 2303 for receiving incoming packets is omitted for clarity). Link quality measurement function 2304 compares the link quality to a threshold for each transmission link and, if necessary, generates an output to weight adjustment function 2305. If a weight adjustment is required, then the weights in table 2306 are adjusted accordingly, preferably according to a gradual (e.g., linearly or exponentially declining) function. In one embodiment, the weight values for all available paths are initially set to the same value, and only when paths degrade in quality are the weights changed to reflect differences.

Link quality measurement function 2304 can be made to operate as part of a synchronizer function as described above. That is, if resynchronization occurs and the receiver detects that synchronization has been lost (e.g., resulting in the synchronization window W being advanced out of sequence), that fact can be used to drive link quality measurement function 2304. According to one embodiment, load balancing is performed using information garnered during the normal synchronization, augmented slightly to communicate link health from the receiver to

the transmitter. The receiver maintains a count, MESS_R(W), of the messages received in synchronization window W. When it receives a synchronization request (SYNC_REQ) corresponding to the end of window W, the receiver includes counter MESS_R in the resulting synchronization acknowledgement (SYNC_ACK) sent back to the transmitter. This allows the transmitter to compare messages sent to messages received in order to asses the health of the link.

If synchronization is completely lost, weight adjustment function 2305 decreases the weight value on the affected path to zero. When synchronization is regained, the weight value for the affected path is gradually increased to its original value. Alternatively, link quality can be measured by evaluating the length of time required for the receiver to acknowledge a synchronization request. In one embodiment, separate transmit and receive tables are used for each transmission path.

When the transmitter receives a SYNC_ACK, the MESS_R is compared with the number of messages transmitted in a window (MESS_T). When the transmitter receives a SYNC_ACK, the traffic probabilities will be examined and adjusted if necessary. MESS_R is compared with the number of messages transmitted in a window (MESS_T). There are two possibilities:

1. If MESS_R is less than a threshold value, THRESH, then the link will be deemed to be unhealthy. If the transmitter was turned off, the transmitter is turned on and the weight P for that link will be set to a minimum value MIN. This will keep a trickle of traffic on the link for monitoring purposes until it recovers. If the transmitter was turned on, the weight P for that link will be set to:

$$P' = \alpha \times MIN + (1 - \alpha) \times P \quad (1)$$

Equation 1 will exponentially damp the traffic weight value to MIN during sustained periods of degraded service.

2. If MESS_R for a link is greater than or equal to THRESH, the link will be deemed healthy. If the weight P for that link is greater than or equal to the steady state value S for that link, then P is left unaltered. If the weight P for that link is less than THRESH then P will be set to:

$$P' = \beta \times S + (1 - \beta) \times P \quad (2)$$

where β is a parameter such that $0<=\beta<=1$ that determines the damping rate of P.

Equation 2 will increase the traffic weight to S during sustained periods of acceptable service in a damped exponential fashion.

A detailed example will now be provided with reference to FIG. 24. As shown in FIG. 24, a first computer 2401 communicates with a second computer 2402 through two routers 2403 and 2404. Each router is coupled to the other router through three transmission links. As described above, these may be physically diverse links or logical links (including virtual private networks).

Suppose that a first link L1 can sustain a transmission bandwidth of 100 Mb/s and has a window size of 32; link L2 can sustain 75 Mb/s and has a window size of 24; and link L3 can sustain 25 Mb/s and has a window size of 8. The combined links can thus sustain 200Mb/s. The steady state traffic weights are 0.5 for link L1; 0.375 for link L2, and 0.125 for link L3. MIN=1Mb/s, THRESH =0.8 MESS_T for each link, α=.75 and β=.5. These traffic weights will remain stable until a link stops for synchronization or reports a number of packets received less than its THRESH. Consider the following sequence of events:

1. Link L1 receives a SYNC_ACK containing a MESS_R of 24, indicating that only 75% of the MESS_T (32) messages transmitted in the last window were successfully received. Link 1 would be below THRESH (0.8). Consequently, link L1's traffic weight value would be reduced to 0.12825, while link L2's traffic weight value would be increased to 0.65812 and link L3's traffic weight value would be increased to 0.217938.

2. Link L2 and L3 remained healthy and link L1 stopped to synchronize. Then link L1's traffic weight value would be set to 0, link L2's traffic weight value would be set to 0.75, and link L33's traffic weight value would be set to 0.25.

3. Link L1 finally received a SYNC_ACK containing a MESS_R of 0 indicating that none of the MESS_T (32) messages transmitted in the last window were successfully received. Link L1 would be below THRESH. Link L1's traffic weight value would be increased to .005, link L2's traffic weight value would be

decreased to 0.74625, and link L3's traffic weight value would be decreased to 0.24875.

4. Link L1 received a SYNC_ACK containing a MESS_R of 32 indicating that 100% of the MESS_T (32) messages transmitted in the last window were successfully received. Link L1 would be above THRESH. Link L1's traffic weight value would be increased to 0.2525, while link L2's traffic weight value would be decreased to 0.560625 and link L3's traffic weight value would be decreased to .186875.

5. Link L1 received a SYNC_ACK containing a MESS_R of 32 indicating that 100% of the MESS_T (32) messages transmitted in the last window were successfully received. Link L1 would be above THRESH. Link L1's traffic weight value would be increased to 0.37625; link L2's traffic weight value would be decreased to 0.4678125, and link L3's traffic weight value would be decreased to 0.1559375.

6. Link L1 remains healthy and the traffic probabilities approach their steady state traffic probabilities.

B. Use of a DNS Proxy to Transparently Create Virtual Private Networks

A second improvement concerns the automatic creation of a virtual private network (VPN) in response to a domain-name server look-up function.

Conventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host. For example, when a computer user types in the web name "Yahoo.com," the user's web browser transmits a request to a DNS, which converts the name into a four-part IP address that is returned to the user's browser and then used by the browser to contact the destination web site.

This conventional scheme is shown in FIG. 25. A user's computer 2501 includes a client application 2504 (for example, a web browser) and an IP protocol stack 2505. When the user enters the name of a destination host, a request DNS REQ is made (through IP protocol stack 2505) to a DNS 2502 to look up the IP address associated with the name. The DNS returns the IP address DNS RESP to client

application 2504, which is then able to use the IP address to communicate with the host 2503 through separate transactions such as PAGE REQ and PAGE RESP.

In the conventional architecture shown in FIG. 25, nefarious listeners on the Internet could intercept the DNS REQ and DNS RESP packets and thus learn what IP addresses the user was contacting. For example, if a user wanted to set up a secure communication path with a web site having the name "Target.com," when the user's browser contacted a DNS to find the IP address for that web site, the true IP address of that web site would be revealed over the Internet as part of the DNS inquiry. This would hamper anonymous communications on the Internet.

One conventional scheme that provides secure virtual private networks over the Internet provides the DNS server with the public keys of the machines that the DNS server has the addresses for. This allows hosts to retrieve automatically the public keys of a host that the host is to communicate with so that the host can set up a VPN without having the user enter the public key of the destination host. One implementation of this standard is presently being developed as part of the FreeS/WAN project(RFC 2535).

The conventional scheme suffers from certain drawbacks. For example, any user can perform a DNS request. Moreover, DNS requests resolve to the same value for all users.

According to certain aspects of the invention, a specialized DNS server traps DNS requests and, if the request is from a special type of user (e.g., one for which secure communication services are defined), the server does not return the true IP address of the target node, but instead automatically sets up a virtual private network between the target node and the user. The VPN is preferably implemented using the IP address "hopping" features of the basic invention described above, such that the true identity of the two nodes cannot be determined even if packets during the communication are intercepted. For DNS requests that are determined to not require secure services (e.g., an unregistered user), the DNS server transparently "passes through" the request to provide a normal look-up function and return the IP address of the target web server, provided that the requesting host has permissions to resolve

unsecured sites. Different users who make an identical DNS request could be provided with different results.

FIG. 26 shows a system employing various principles summarized above. A user's computer 2601 includes a conventional client (e.g., a web browser) 2605 and an IP protocol stack 2606 that preferably operates in accordance with an IP hopping function 2607 as outlined above. A modified DNS server 2602 includes a conventional DNS server function 2609 and a DNS proxy 2610. A gatekeeper server 2603 is interposed between the modified DNS server and a secure target site 2704. An "unsecure" target site 2611 is also accessible via conventional IP protocols.

According to one embodiment, DNS proxy 2610 intercepts all DNS lookup functions from client 2605 and determines whether access to a secure site has been requested. If access to a secure site has been requested (as determined, for example, by a domain name extension, or by reference to an internal table of such sites), DNS proxy 2610 determines whether the user has sufficient security privileges to access the site. If so, DNS proxy 2610 transmits a message to gatekeeper 2603 requesting that a virtual private network be created between user computer 2601 and secure target site 2604. In one embodiment, gatekeeper 2603 creates "hopblocks" to be used by computer 2601 and secure target site 2604 for secure communication. Then, gatekeeper 2603 communicates these to user computer 2601. Thereafter, DNS proxy 2610 returns to user computer 2601 the resolved address passed to it by the gatekeeper (this address could be different from the actual target computer) 2604, preferably using a secure administrative VPN. The address that is returned need not be the actual address of the destination computer.

Had the user requested lookup of a non-secure web site such as site 2611, DNS proxy would merely pass through to conventional DNS server 2609 the look-up request, which would be handled in a conventional manner, returning the IP address of non-secure web site 2611. If the user had requested lookup of a secure web site but lacked credentials to create such a connection, DNS proxy 2610 would return a "host unknown" error to the user. In this manner, different users requesting access to the same DNS name could be provided with different look-up results.

Gatekeeper 2603 can be implemented on a separate computer (as shown in FIG. 26) or as a function within modified DNS server 2602. In general, it is anticipated that gatekeeper 2703 facilitates the allocation and exchange of information needed to communicate securely, such as using "hopped" IP addresses. Secure hosts such as site 2604 are assumed to be equipped with a secure communication function such as an IP hopping function 2608.

It will be appreciated that the functions of DNS proxy 2610 and DNS server 2609 can be combined into a single server for convenience. Moreover, although element 2602 is shown as combining the functions of two servers, the two servers can be made to operate independently.

FIG. 27 shows steps that can be executed by DNS proxy server 2610 to handle requests for DNS look-up for secure hosts. In step 2701, a DNS look-up request is received for a target host. In step 2702, a check is made to determine whether access to a secure host was requested. If not, then in step 2703 the DNS request is passed to conventional DNS server 2609, which looks up the IP address of the target site and returns it to the user's application for further processing.

In step 2702, if access to a secure host was requested, then in step 2704 a further check is made to determine whether the user is authorized to connect to the secure host. Such a check can be made with reference to an internally stored list of authorized IP addresses, or can be made by communicating with gatekeeper 2603 (e.g., over an "administrative" VPN that is secure). It will be appreciated that different levels of security can also be provided for different categories of hosts. For example, some sites may be designated as having a certain security level, and the security level of the user requesting access must match that security level. The user's security level can also be determined by transmitting a request message back to the user's computer requiring that it prove that it has sufficient privileges.

If the user is not authorized to access the secure site, then a "host unknown" message is returned (step 2705). If the user has sufficient security privileges, then in step 2706 a secure VPN is established between the user's computer and the secure target site. As described above, this is preferably done by allocating a hopping regime

that will be carried out between the user's computer and the secure target site, and is preferably performed transparently to the user (i.e., the user need not be involved in creating the secure link). As described in various embodiments of this application, any of various fields can be "hopped" (e.g., IP source/destination addresses; a field in the header; etc.) in order to communicate securely.

Some or all of the security functions can be embedded in gatekeeper 2603, such that it handles all requests to connect to secure sites. In this embodiment, DNS proxy 2610 communicates with gatekeeper 2603 to determine (preferably over a secure administrative VPN) whether the user has access to a particular web site.

Various scenarios for implementing these features are described by way of example below:

Scenario #1: Client has permission to access target computer, and gatekeeper has a rule to make a VPN for the client. In this scenario, the client's DNS request would be received by the DNS proxy server 2610, which would forward the request to gatekeeper 2603. The gatekeeper would establish a VPN between the client and the requested target. The gatekeeper would provide the address of the destination to the DNS proxy, which would then return the resolved name as a result. The resolved address can be transmitted back to the client in a secure administrative VPN.

Scenario #2: Client does not have permission to access target computer. In this scenario, the client's DNS request would be received by the DNS proxy server 2610, which would forward the request to gatekeeper 2603. The gatekeeper would reject the request, informing DNS proxy server 2610 that it was unable to find the target computer. The DNS proxy 2610 would then return a "host unknown" error message to the client.

Scenario #3: Client has permission to connect using a normal non-VPN link, and the gatekeeper does not have a rule to set up a VPN for the client to the target site. In this scenario, the client's DNS request is received by DNS proxy server 2610, which would check its rules and determine that no VPN is needed. Gatekeeper 2603 would then inform the DNS proxy server to forward the request to conventional DNS

server 2609, which would resolve the request and return the result to the DNS proxy server and then back to the client.

Scenario #4: Client does not have permission to establish a normal/non-VPN link, and the gatekeeper does not have a rule to make a VPN for the client to the target site. In this scenario, the DNS proxy server would receive the client's DNS request and forward it to gatekeeper 2603. Gatekeeper 2603 would determine that no special VPN was needed, but that the client is not authorized to communicate with non-VPN members. The gatekeeper would reject the request, causing DNS proxy server 2610 to return an error message to the client.

C. Large Link to Small Link Bandwidth Management

One feature of the basic architecture is the ability to prevent so-called "denial of service" attacks that can occur if a computer hacker floods a known Internet node with packets, thus preventing the node from communicating with other nodes. Because IP addresses or other fields are "hopped" and packets arriving with invalid addresses are quickly discarded, Internet nodes are protected against flooding targeted at a single IP address.

In a system in which a computer is coupled through a link having a limited bandwidth (e.g., an edge router) to a node that can support a much higher-bandwidth link (e.g., an Internet Service Provider), a potential weakness could be exploited by a determined hacker. Referring to FIG. 28. suppose that a first host computer 2801 is communicating with a second host computer 2804 using the IP address hopping principles described above. The first host computer is coupled through an edge router 2802 to an Internet Service Provider (ISP) 2803 through a low bandwidth link (LOW BW), and is in turn coupled to second host computer 2804 through parts of the Internet through a high bandwidth link (HIGH BW). In this architecture, the ISP is able to support a high bandwidth to the internet, but a much lower bandwidth to the edge router 2802.

Suppose that a computer hacker is able to transmit a large quantity of dummy packets addressed to first host computer 2801 across high bandwidth link HIGH BW. Normally, host computer 2801 would be able to quickly reject the packets since they

would not fall within the acceptance window permitted by the IP address hopping scheme. However, because the packets must travel across low bandwidth link LOW BW, the packets overwhelm the lower bandwidth link before they are received by host computer 2801. Consequently, the link to host computer 2801 is effectively flooded before the packets can be discarded.

According to one inventive improvement, a "link guard" function 2805 is inserted into the high-bandwidth node (e.g., ISP 2803) that quickly discards packets destined for a low-bandwidth target node if they are not valid packets. Each packet destined for a low-bandwidth node is cryptographically authenticated to determine whether it belongs to a VPN. If it is not a valid VPN packet, the packet is discarded at the high-bandwidth node. If the packet is authenticated as belonging to a VPN, the packet is passed with high preference. If the packet is a valid non-VPN packet, it is passed with a lower quality of service (e.g., lower priority).

In one embodiment, the ISP distinguishes between VPN and non-VPN packets using the protocol of the packet. In the case of IPSEC [rfc 2401], the packets have IP protocols 420 and 421. In the case of the TARP VPN, the packets will have an IP protocol that is not yet defined. The ISP's link guard, 2805, maintains a table of valid VPNs which it uses to validate whether VPN packets are cryptographically valid.

According to one embodiment, packets that do not fall within any hop windows used by nodes on the low-bandwidth link are rejected, or are sent with a lower quality of service. One approach for doing this is to provide a copy of the IP hopping tables used by the low-bandwidth nodes to the high-bandwidth node, such that both the high-bandwidth and low-bandwidth nodes track hopped packets (e.g., the high-bandwidth node moves its hopping window as valid packets are received). In such a scenario, the high-bandwidth node discards packets that do not fall within the hopping window before they are transmitted over the low-bandwidth link. Thus, for example, ISP 2903 maintains a copy 2910 of the receive table used by host computer 2901. Incoming packets that do not fall within this receive table are discarded. According to a different embodiment, link guard 2805 validates each VPN packet using a keyed hashed message authentication code (HMAC) [rfc 2104]. According

to another embodiment, separate VPNs (using, for example, hopblocks) can be established for communicating between the low-bandwidth node and the high-bandwidth node (i.e., packets arriving at the high-bandwidth node are converted into different packets before being transmitted to the low-bandwidth node).

As shown in FIG. 29, for example, suppose that a first host computer 2900 is communicating with a second host computer 2902 over the Internet, and the path includes a high bandwidth link HIGH BW to an ISP 2901 and a low bandwidth link LOW BW through an edge router 2904. In accordance with the basic architecture described above, first host computer 2900 and second host computer 2902 would exchange hopblocks (or a hopblock algorithm) and would be able to create matching transmit and receive tables 2905, 2906, 2912 and 2913. Then in accordance with the basic architecture, the two computers would transmit packets having seemingly random IP source and destination addresses, and each would move a corresponding hopping window in its receive table as valid packets were received.

Suppose that a nefarious computer hacker 2903 was able to deduce that packets having a certain range of IP addresses (e.g., addresses 100 to 200 for the sake of simplicity) are being transmitted to ISP 2901, and that these packets are being forwarded over a low-bandwidth link. Hacker computer 2903 could thus "flood" packets having addresses falling into the range 100 to 200, expecting that they would be forwarded along low bandwidth link LOW BW, thus causing the low bandwidth link to become overwhelmed. The fast packet reject mechanism in first host computer 3000 would be of little use in rejecting these packets, since the low bandwidth link was effectively jammed before the packets could be rejected. In accordance with one aspect of the improvement, however, VPN link guard 2911 would prevent the attack from impacting the performance of VPN traffic because the packets would either be rejected as invalid VPN packets or given a lower quality of service than VPN traffic over the lower bandwidth link. A denial-of-service flood attack could, however, still disrupt non-VPN traffic.

According to one embodiment of the improvement, ISP 2901 maintains a separate VPN with first host computer 2900, and thus translates packets arriving at the

ISP into packets having a different IP header before they are transmitted to host computer 2900. The cryptographic keys used to authenticate VPN packets at the link guard 2911 and the cryptographic keys used to encrypt and decrypt the VPN packets at host 2902 and host 2901 can be different, so that link guard 2911 does not have access to the private host data; it only has the capability to authenticate those packets.

According to yet a third embodiment, the low-bandwidth node can transmit a special message to the high-bandwidth node instructing it to shut down all transmissions on a particular IP address, such that only hopped packets will pass through to the low-bandwidth node. This embodiment would prevent a hacker from flooding packets using a single IP address. According to yet a fourth embodiment, the high-bandwidth node can be configured to discard packets transmitted to the low-bandwidth node if the transmission rate exceeds a certain predetermined threshold for any given IP address; this would allow hopped packets to go through. In this respect, link guard 2911 can be used to detect that the rate of packets on a given IP address are exceeding a threshold rate; further packets addressed to that same IP address would be dropped or transmitted at a lower priority (e.g., delayed).

D. Traffic Limiter

In a system in which multiple nodes are communicating using "hopping" technology, a treasonous insider could internally flood the system with packets. In order to prevent this possibility, one inventive improvement involves setting up "contracts" between nodes in the system, such that a receiver can impose a bandwidth limitation on each packet sender. One technique for doing this is to delay acceptance of a checkpoint synchronization request from a sender until a certain time period (e.g., one minute) has elapsed. Each receiver can effectively control the rate at which its hopping window moves by delaying "SYNC ACK" responses to "SYNC_REQ" messages.

A simple modification to the checkpoint synchronizer will serve to protect a receiver from accidental or deliberate overload from an internally treasonous client. This modification is based on the observation that a receiver will not update its tables until a SYNC_REQ is received on hopped address CKPT_N. It is a simple matter of

deferring the generation of a new CKPT_N until an appropriate interval after previous checkpoints.

Suppose a receiver wished to restrict reception from a transmitter to 100 packets a second, and that checkpoint synchronization messages were triggered every 50 packets. A compliant transmitter would not issue new SYNC_REQ messages more often than every 0.5 seconds. The receiver could delay a non-compliant transmitter from synchronizing by delaying the issuance of CKPT_N for 0.5 second after the last SYNC_REQ was accepted.

In general, if M receivers need to restrict N transmitters issuing new SYNC_REQ messages after every W messages to sending R messages a second in aggregate. each receiver could defer issuing a new CKPT_N until MxNxW/R seconds have elapsed since the last SYNC_REQ has been received and accepted. If the transmitter exceeds this rate between a pair of checkpoints, it will issue the new checkpoint before the receiver is ready to receive it, and the SYNC_REQ will be discarded by the receiver. After this, the transmitter will re-issue the SYNC_REQ every T1 seconds until it receives a SYNC_ACK. The receiver will eventually update CKPT_N and the SYNC_REQ will be acknowledged. If the transmission rate greatly exceeds the allowed rate, the transmitter will stop until it is compliant. If the transmitter exceeds the allowed rate by a little, it will eventually stop after several rounds of delayed synchronization until it is in compliance. Hacking the transmitter's code to not shut off only permits the transmitter to lose the acceptance window. In this case it can recover the window and proceed only after it is compliant again.

Two practical issues should be considered when implementing the above scheme:

1. The receiver rate should be slightly higher than the permitted rate in order to allow for statistical fluctuations in traffic arrival times and non-uniform load balancing.

2. Since a transmitter will rightfully continue to transmit for a period after a SYNC_REQ is transmitted, the algorithm above can artificially reduce the transmitter's bandwidth. If events prevent a compliant transmitter from synchronizing

for a period (e.g. the network dropping a SYNC_REQ or a SYNC_ACK) a SYNC_REQ will be accepted later than expected. After this, the transmitter will transmit fewer than expected messages before encountering the next checkpoint. The new checkpoint will not have been activated and the transmitter will have to retransmit the SYNC_REQ. This will appear to the receiver as if the transmitter is not compliant. Therefore, the next checkpoint will be accepted late from the transmitter's perspective. This has the effect of reducing the transmitter's allowed packet rate until the transmitter transmits at a packet rate below the agreed upon rate for a period of time.

To guard against this, the receiver should keep track of the times that the last C SYNC_REQs were received and accepted and use the minimum of MxNxW/R seconds after the last SYNC_REQ has been received and accepted, 2xMxNxW/R seconds after next to the last SYNC_REQ has been received and accepted, CxMxNxW/R seconds after $(C-1)^{th}$ to the last SYNC_REQ has been received, as the time to activate CKPT_N. This prevents the receiver from inappropriately limiting the transmitter's packet rate if at least one out of the last C SYNC_REQs was processed on the first attempt.

FIG. 30 shows a system employing the above-described principles. In FIG. 30, two computers 3000 and 3001 are assumed to be communicating over a network N in accordance with the "hopping" principles described above (e.g., hopped IP addresses, discriminator values, etc.). For the sake of simplicity, computer 3000 will be referred to as the receiving computer and computer 3001 will be referred to as the transmitting computer, although full duplex operation is of course contemplated. Moreover, although only a single transmitter is shown, multiple transmitters can transmit to receiver 3000.

As described above, receiving computer 3000 maintains a receive table 3002 including a window W that defines valid IP address pairs that will be accepted when appearing in incoming data packets. Transmitting computer 3001 maintains a transmit table 3003 from which the next IP address pairs will be selected when transmitting a packet to receiving computer 3000. (For the sake of illustration,

window W is also illustrated with reference to transmit table 3003). As transmitting computer moves through its table, it will eventually generate a SYNC_REQ message as illustrated in function 3010. This is a request to receiver 3000 to synchronize the receive table 3002, from which transmitter 3001 expects a response in the form of a CKPT_N (included as part of a SYNC_ACK message). If transmitting computer 3001 transmits more messages than its allotment, it will prematurely generate the SYNC_REQ message. (If it has been altered to remove the SYNC_REQ message generation altogether, it will fall out of synchronization since receiver 3000 will quickly reject packets that fall outside of window W, and the extra packets generated by transmitter 3001 will be discarded).

In accordance with the improvements described above, receiving computer 3000 performs certain steps when a SYNC_REQ message is received, as illustrated in FIG. 30. In step 3004, receiving computer 3000 receives the SYNC_REQ message. In step 3005, a check is made to determine whether the request is a duplicate. If so, it is discarded in step 3006. In step 3007, a check is made to determine whether the SYNC_REQ received from transmitter 3001 was received at a rate that exceeds the allowable rate R (i.e., the period between the time of the last SYNC_REQ message). The value R can be a constant, or it can be made to fluctuate as desired. If the rate exceeds R, then in step 3008 the next activation of the next CKPT_N hopping table entry is delayed by W/R seconds after the last SYNC_REQ has been accepted.

Otherwise, if the rate has not been exceeded, then in step 3109 the next CKPT_N value is calculated and inserted into the receiver's hopping table prior to the next SYNC_REQ from thetransmitter 3101. Transmitter 3101 then processes the SYNC_REQ in the normal manner.

E. Signaling Synchronizer

In a system in which a large number of users communicate with a central node using secure hopping technology, a large amount of memory must be set aside for hopping tables and their supporting data structures. For example, if one million subscribers to a web site occasionally communicate with the web site, the site must maintain one million hopping tables, thus using up valuable computer resources, even

though only a small percentage of the users may actually be using the system at any one time. A desirable solution would be a system that permits a certain maximum number of simultaneous links to be maintained, but which would "recognize" millions of registered users at any one time. In other words, out of a population of a million registered users, a few thousand at a time could simultaneously communicate with a central server, without requiring that the server maintain one million hopping tables of appreciable size.

One solution is to partition the central node into two nodes: a signaling server that performs session initiation for user log-on and log-off (and requires only minimally sized tables), and a transport server that contains larger hopping tables for the users. The signaling server listens for the millions of known users and performs a fast-packet reject of other (bogus) packets. When a packet is received from a known user, the signaling server activates a virtual private link (VPL) between the user and the transport server, where hopping tables are allocated and maintained. When the user logs onto the signaling server, the user's computer is provided with hop tables for communicating with the transport server, thus activating the VPL. The VPLs can be torn down when they become inactive for a time period, or they can be torn down upon user log-out. Communication with the signaling server to allow user log-on and log-off can be accomplished using a specialized version of the checkpoint scheme described above.

FIG. 31 shows a system employing certain of the above-described principles. In FIG. 31, a signaling server 3101 and a transport server 3102 communicate over a link. Signaling server 3101 contains a large number of small tables 3106 and 3107 that contain enough information to authenticate a communication request with one or more clients 3103 and 3104. As described in more detail below, these small tables may advantageously be constructed as a special case of the synchronizing checkpoint tables described previously. Transport server 3102, which is preferably a separate computer in communication with signaling server 3101, contains a smaller number of larger hopping tables 3108, 3109, and 3110 that can be allocated to create a VPN with one of the client computers.

According to one embodiment, a client that has previously registered with the system (e.g., via a system administration function, a user registration procedure, or some other method) transmits a request for information from a computer (e.g., a web site). In one variation, the request is made using a "hopped" packet, such that signaling server 3101 will quickly reject invalid packets from unauthorized computers such as hacker computer 3105. An "administrative" VPN can be established between all of the clients and the signaling server in order to ensure that a hacker cannot flood signaling server 3101 with bogus packets. Details of this scheme are provided below.

Signaling server 3101 receives the request 3111 and uses it to determine that client 3103 is a validly registered user. Next, signaling server 3101 issues a request to transport server 3102 to allocate a hopping table (or hopping algorithm or other regime) for the purpose of creating a VPN with client 3103. The allocated hopping parameters are returned to signaling server 3101 (path 3113), which then supplies the hopping parameters to client 3103 via path 3114, preferably in encrypted form.

Thereafter, client 3103 communicates with transport server 3102 using the normal hopping techniques described above. It will be appreciated that although signaling server 3101 and transport server 3102 are illustrated as being two separate computers, they could of course be combined into a single computer and their functions performed on the single computer. Alternatively, it is possible to partition the functions shown in FIG. 31 differently from as shown without departing from the inventive principles.

One advantage of the above-described architecture is that signaling server 3101 need only maintain a small amount of information on a large number of potential users, yet it retains the capability of quickly rejecting packets from unauthorized users such as hacker computer 3105. Larger data tables needed to perform the hopping and synchronization functions are instead maintained in a transport server 3102, and a smaller number of these tables are needed since they are only allocated for "active" links. After a VPN has become inactive for a certain time period (e.g., one hour), the VPN can be automatically torn down by transport server 3102 or signaling server 3101.

A more detailed description will now be provided regarding how a special case of the checkpoint synchronization feature can be used to implement the signaling scheme described above.

The signaling synchronizer may be required to support many (millions) of standing, low bandwidth connections. It therefore should minimize per-VPL memory usage while providing the security offered by hopping technology. In order to reduce memory usage in the signaling server, the data hopping tables can be completely eliminated and data can be carried as part of the SYNC_REQ message. The table used by the server side (receiver) and client side (transmitter) is shown schematically as element 3106 in FIG. 31.

The meaning and behaviors of CKPT_N, CKPT_O and CKPT_R remain the same from the previous description, except that CKPT_N can receive a combined data and SYNC_REQ message or a SYNC_REQ message without the data.

The protocol is a straightforward extension of the earlier synchronizer. Assume that a client transmitter is on and the tables are synchronized. The initial tables can be generated "out of band." For example, a client can log into a web server to establish an account over the Internet. The client will receive keys etc encrypted over the Internet. Meanwhile, the server will set up the signaling VPN on the signaling server.

Assuming that a client application wishes to send a packet to the server on the client's standing signaling VPL:

1. The client sends the message marked as a data message on the inner header using the transmitter's CKPT_N address. It turns the transmitter off and starts a timer T1 noting CKPT_O. Messages can be one of three types: DATA, SYNC_REQ and SYNC_ACK. In the normal algorithm, some potential problems can be prevented by identifying each message type as part of the encrypted inner header field. In this algorithm, it is important to distinguish a data packet and a SYNC_REQ in the signaling synchronizer since the data and the SYNC_REQ come in on the same address.

2. When the server receives a data message on its CKPT_N, it verifies the message and passes it up the stack. The message can be verified by checking message type and and other information (i.e user credentials) contained in the inner header It replaces its CKPT_O with CKPT_N and generates the next CKPT_N. It updates its transmitter side CKPT_R to correspond to the client's receiver side CKPT_R and transmits a SYNC_ACK containing CKPT_O in its payload.

3. When the client side receiver receives a SYNC_ACK on its CKPT_R with a payload matching its transmitter side CKPT_O and the transmitter is off, the transmitter is turned on and the receiver side CKPT_R is updated. If the SYNC_ACK's payload does not match the transmitter side CKPT_O or the transmitter is on, the SYNC_ACK is simply discarded.

4. T1 expires: If the transmitter is off and the client's transmitter side CKPT_O matches the CKPT_O associated with the timer, it starts timer T1 noting CKPT_O again, and a SYNC_REQ is sent using the transmitter's CKPT_O address. Otherwise, no action is taken.

5. When the server receives a SYNC_REQ on its CKPT_N, it replaces its CKPT_O with CKPT_N and generates the next CKPT_N. It updates its transmitter side CKPT_R to correspond to the client's receiver side CKPT_R and transmits a SYNC_ACK containing CKPT_O in its payload.

6. When the server receives a SYNC_REQ on its CKPT_O, it updates its transmitter side CKPT_R to correspond to the client's receiver side CKPT_R and transmits a SYNC_ACK containing CKPT_O in its payload.

FIG. 32 shows message flows to highlight the protocol. Reading from top to bottom, the client sends data to the server using its transmitter side CKPT_N. The client side transmitter is turned off and a retry timer is turned off. The transmitter will not transmit messages as long as the transmitter is turned off. The client side transmitter then loads CKPT_N into CKPT_O and updates CKPT_N. This message is successfully received and a passed up the stack. It also synchronizes the receiver i.e, the server loads CKPT_N into CKPT_O and generates a new CKPT_N, it generates a new CKPT_R in the server side transmitter and transmits a SYNC_ACK containing

the server side receiver's CKPT_O the server. The SYNC_ACK is successfully received at the client. The client side receiver's CKPT_R is updated, the transmitter is turned on and the retry timer is killed. The client side transmitter is ready to transmit a new data message.

Next, the client sends data to the server using its transmitter side CKPT_N. The client side transmitter is turned off and a retry timer is turned off. The transmitter will not transmit messages as long as the transmitter is turned off. The client side transmitter then loads CKPT_N into CKPT_O and updates CKPT_N. This message is lost. The client side timer expires and as a result a SYNC_REQ is transmitted on the client side transmitter's CKPT_O (this will keep happening until the SYNC_ACK has been received at the client). The SYNC_REQ is successfully received at the server. It synchronizes the receiver i.e, the server loads CKPT_N into CKPT_O and generates a new CKPT_N, it generates an new CKPT_R in the server side transmitter and transmits a SYNC_ACK containing the server side receiver's CKPT_O the server. The SYNC_ACK is successfully received at the client. The client side receiver's CKPT_R is updated, the transmitter is turned off and the retry timer is killed. The client side transmitter is ready to transmit a new data message.

There are numerous other scenarios that follow this flow. For example, the SYNC_ACK could be lost. The transmitter would continue to re-send the SYNC_REQ until the receiver synchronizes and responds.

The above-described procedures allow a client to be authenticated at signaling server 3201 while maintaining the ability of signaling server 3201 to quickly reject invalid packets, such as might be generated by hacker computer 3205. In various embodiments, the signaling synchronizer is really a derivative of the synchronizer. It provides the same protection as the hopping protocol, and it does so for a large number of low bandwidth connections.

CLAIMS

1. A method of transmitting data packets between a first computer and a second computer, wherein the first computer and the second computer are linked via a plurality of separate transmission paths, the method comprising the steps of:

(1) assigning a weight value to each of the plurality of transmission paths, wherein each respective weight value represents the relative number of packets that a respective transmission path will transmit;

(2) for each data packet that is to be transmitted from the first computer to the second computer, selecting one of the plurality of transmission paths on the basis of each respective transmission path's assigned weight value;

(3) measuring the transmission quality for each of the plurality of transmission paths; and

(4) adjusting downwardly to a non-zero value the assigned weight value for a transmission path for which the transmission quality has declined.

2. The method of claim 1, wherein step (4) comprises the step of gradually decreasing over time the assigned weight value in relation to weight values assigned to the remaining transmission paths.

3. The method of claim 2, wherein step (4) comprises the step of gradually decreasing the assigned weight value according to an incrementally decreasing function.

4. The method of claim 2, wherein step (4) comprises the step of gradually decreasing the assigned weight value according to an exponentially decaying function.

5. The method of claim 1, wherein step (3) comprises the step of determining that one or more packets transmitted to the second computer was not acknowledged by the second computer.

6. The method of claim 1, wherein step (3) comprises the step of evaluating the contents of a synchronization packet that maintains synchronization with a moving window of valid values.

7. The method of claim 1, further comprising the step of inserting into each data packet a source and destination IP address pair that is selected according to a pseudo-random sequence.

8. The method of claim 1, wherein step (4) comprises the step of adjusting downwardly the assigned weight value for a transmission path only if the transmission quality has declined below a predetermined threshold.

9. The method of claim 1, further comprising the step of adjusting upwardly the assigned weight value that was adjusted in step (4) if it is later determined that the transmission quality has improved.

10. The method of claim 1, further comprising the step of adjusting upwardly the weight values of the remaining transmission links in an amount that compensates for the downwardly adjusted weight value.

11. The method of claim 10, wherein the step of adjusting upwardly comprises the step of equally distributing the amount that was downwardly adjusted across the remaining transmission links.

12. The method of claim 1, further comprising the step of adjusting downwardly to zero the assigned weight value for any transmission link whose quality has degraded below a preset threshold.

13. The method of claim 1, wherein steps (2) through (4) are repeated periodically.

14. A first computer that transmits data packets to a second computer over a plurality of separate transmission paths, wherein the first computer performs the steps of:

(1) assigning a weight value to each of the plurality of transmission paths, wherein each respective weight value represents the relative number of packets that a respective transmission path will transmit;

(2) for each data packet that is to be transmitted to the second computer, selecting one of the plurality of transmission paths on the basis of each respective transmission path's assigned weight value;

(3) measuring the transmission quality for each of the plurality of transmission paths; and

(4) adjusting downwardly to a non-zero value the assigned weight value for a transmission path for which the transmission quality has declined.

15. The first computer of claim 14, wherein the first computer gradually decreases over time the assigned weight value in relation to weight values assigned to the remaining transmission paths.

16. The first computer of claim 15, wherein the first computer gradually decreases the assigned weight value according to an incrementally decreasing function.

17. The first computer of claim 15, wherein the first computer gradually decreases the assigned weight value according to an exponentially decaying function.

18. The first computer of claim 14, wherein the first computer measures the transmission quality by determining that one or more packets transmitted to the second computer was not acknowledged by the second computer.

19. The first computer of claim 14, wherein the first computer measures the transmission quality by evaluating the contents of a synchronization packet that maintains synchronization with a moving window of valid values.

20. The first computer of claim 14, wherein the first computer inserts into each data packet a source and destination IP address pair that is selected according to a pseudo-random sequence.

21. The first computer of claim 14, wherein the first computer adjusts downwardly the assigned weight value for any transmission path only if the transmission quality has declined below a predetermined threshold.

22. The first computer of claim 14, wherein the first computer adjusts upwardly the assigned weight value that was adjusted in step (4) if it is later determined that the transmission quality has improved.

23. The first computer of claim 14, wherein the first computer adjusts upwardly the weight values of the remaining transmission links in an amount that compensates for the downwardly adjusted weight value.

24. The first computer of claim 23, wherein the first computer upwardly adjusts probabilities across the remaining transmission links in an amount equal to the downwardly adjusted weight value.

25. The first computer of claim 14, wherein the first computer adjusts downwardly to zero the assigned weight value for any transmission link whose quality has degraded below a preset threshold.

26. The first computer of claim 14, wherein the first computer repeats steps (2) through (4) periodically.

27. A system comprising the first computer of claim 14 and a second computer constructed in accordance with the first computer of claim 14.

28. A method of transparently creating a virtual private network (VPN) between a client computer and a target computer, comprising the steps of:

(1) generating from the client computer a Domain Name Service (DNS) request that requests an IP address corresponding to a domain name associated with the target computer;

(2) determining whether the DNS request transmitted in step (1) is requesting access to a secure web site; and

(3) in response to determining that the DNS request in step (2) is requesting access to a secure target web site, automatically initiating the VPN between the client computer and the target computer.

29. The method of claim 28, wherein steps (2) and (3) are performed at a DNS server separate from the client computer.

30. The method of claim 28, further comprising the step of:

(4) in response to determining that the DNS request in step (2) is not requesting access to a secure target web site, resolving the IP address for the domain name and returning the IP address to the client computer.

31. The method of claim 28, wherein step (3) comprises the step of, prior to automatically initiating the VPN between the client computer and the target computer, determining whether the client computer is authorized to establish a VPN with the target computer and, if not so authorized, returning an error from the DNS request.

32. The method of claim 28, wherein step (3) comprises the step of, prior to automatically initiating the VPN between the client computer and the target computer, determining whether the client computer is authorized to resolve addresses of non secure target computers and, if not so authorized, returning an error from the DNS request.

33. The method of claim 28, wherein step (3) comprises the step of establishing the VPN by creating an IP address hopping scheme between the client computer and the target computer.

34. The method of claim 28, wherein step (3) comprises the step of using a gatekeeper computer that allocates VPN resources for communicating between the client computer and the target computer.

35. The method of claim 28, wherein step (2) is performed in a DNS proxy server that passes through the request to a DNS server if it is determined in step (3) that access is not being requested to a secure target web site.

36. The method of claim 32, wherein step (3) comprises the step of transmitting a message to the client computer to determine whether the client computer is authorized to establish the VPN target computer.

37. A system that transparently creates a virtual private network (VPN) between a client computer and a secure target computer, comprising:

a DNS proxy server that receives a request from the client computer to look up an IP address for a domain name, wherein the DNS proxy server returns the IP address for the requested domain name if it is determined that access to a non-secure web site has been requested, and wherein the DNS proxy server generates a request to create the VPN between the client computer and the secure target computer if it is determined that access to a secure web site has been requested; and

a gatekeeper computer that allocates resources for the VPN between the client computer and the secure web computer in response to the request by the DNS proxy server.

38. The system of claim 37, wherein the gatekeeper computer creates the VPN by establishing an IP address hopping regime that is used to pseudorandomly

change IP addresses in packets transmitted between the client computer and the secure target computer.

39. The system of claim 37, wherein the gatekeeper computer determines whether the client computer has sufficient security privileges to create the VPN and, if the client computer lacks sufficient security privileges, rejecting the request to create the VPN.

40. A method of preventing data packets received from a high bandwidth link from flooding a low bandwidth link, comprising the steps of:

(1) receiving data packets from the high bandwidth link that are ostensibly addressed to a computer residing on the low-bandwidth link;

(2) for each data packet, determining whether the data packet is validly addressed to the computer on the low-bandwidth link;

(3) in response to determining that the data packet is not validly addressed to the computer on the low-bandwidth link, rejecting the data packet; and

(4) in response to determining that the data packet is validly addressed to the computer on the low-bandwidth link, forwarding the data packet to the computer over the low-bandwidth link.

41. The method of claim 40, wherein step (3) comprises the step of comparing a value in a header of each data packet to a set of valid values maintained for the computer on the low-bandwidth link.

42. The method of claim 41, wherein step (3) comprises the step of comparing a value in a header of each data packet to a moving window of valid values.

43. The method of claim 42, wherein step (3) comprises the step of comparing the IP address in the header of each data packet to a moving window of valid IP addresses, wherein the moving window is also maintained by the computer on the low-bandwidth link.

44. The method of claim 40, wherein step (3) comprises the step of reducing a priority level of the packet in relation to other data packets, wherein the priority level determines whether a particular data packet will be transmitted before another data packet having a different priority level.

45. The method of claim 40, wherein step (3) comprises the step of performing a cryptographic check on each data packet to determine whether each data packet is validly addressed.

46. The method of claim 40, wherein step (3) comprises the step of receiving a message from the computer on the low-bandwidth link to stop accepting messages having a particular characteristic.

47. The method of claim 46, wherein step (3) comprises the step of receiving a message from the computer on the low-bandwidth link to stop accepting messages addressed to a particular IP address.

48. The method of claim 40, wherein step (3) comprises the step of determining that a packet transmission rate has been exceeded for a given packet parameter.

49. The method of claim 48, wherein step (3) comprises the step of determining that a packet transmission rate has been exceeded for a given IP destination address.

50. In a system having a low bandwidth data link, a first computer coupled to the low bandwidth data link, and a high bandwidth data link, an improvement comprising:

a second computer coupled between the low bandwidth data link and the high bandwidth data link, wherein the second computer receives data packets from the high bandwidth data link and, if they are addressed to the first computer, routes them to the first computer over the low bandwidth data link,

wherein the second computer prevents invalid data packets ostensibly addressed to the first computer from being transmitted over the low bandwidth data link.

51. The system of claim 50, wherein the second computer prevents invalid data packets from being transmitted over the low bandwidth data link by comparing a discriminator field in a header of each data packet to a table of valid discriminator fields maintained for the first computer.

52. The system of claim 50, wherein the second computer compares an Internet Protocol (IP) address in a header of each data packet to a table of valid IP addresses.

53. The system of claim 52, wherein the second computer compares the IP address in the header of each data packet to a moving window of valid IP addresses, wherein the moving window is also maintained by the first computer.

54. The system of claim 50, wherein the second computer reduces a priority level of a data packet in relation to other data packets, wherein the priority level determines whether a particular data packet will be transmitted before another data packet having a different priority level.

55. The system of claim 50, wherein the second computer performs a cryptographic check on each data packet to determine whether each data packet is validly addressed.

56. The system of claim 50, wherein the second computer receives a message from the first computer that causes the second computer to stop accepting messages having a particular characteristic.

57. The system of claim 56, wherein the second computer receiving a message from the first computer to stop accepting messages addressed to a particular IP address.

58. The system of claim 50, wherein the second computer rejects invalid packets by determining that a packet transmission rate has been exceeded for a given packet parameter.

59. The system of claim 58, wherein the second computer determines that a packet transmission rate has been exceeded for a given IP destination address.

60. In a system comprising a first computer that transmits data packets to a second computer over a network according to a scheme by which at least one field in a series of data packets is periodically changed according to a sequence known by the first and second computers, and wherein the second computer periodically receives a synchronization request from the first computer to maintain synchronization of the sequence between the first and second computers, a method comprising the steps of:

(1) receiving at the first computer the synchronization request from the second computer;

(2) determining whether the synchronization request was received in less than a predetermined interval;

(3) in response to determining that the synchronization request was received in less than the predetermined interval, ignoring the synchronization request; and

(4) in response to determining that the synchronization request was not received in less than the predetermined interval, providing the synchronization response to the first computer.

61. The method of claim 60, wherein step (3) comprises the step of delaying the acceptance of a SYNC_REQ for W/R seconds, where W is the number of data packets between synchronization requests according to an agreed schedule, and R is the agreed rate at which synchronization requests should be received according to the agreed schedule.

62. The method of claim 60, further comprising the step of determining whether the synchronization request is a duplicate of a previously received synchronization request and, if it is a duplicate, discarding it.

63. The method of claim 60, wherein step (4) comprises the step of providing a response that includes a new checkpoint for synchronizing a window in a hopping table.

64. A computer that receives data packets from a second computer over a network according to a scheme by which at least one field in a series of data packets is periodically changed according to a known sequence, wherein the second computer periodically transmits a synchronization request to maintain synchronization of the sequence, wherein the computer performs the steps of:

(1) receiving the synchronization request from the second computer;

(2) determining whether the synchronization request was received in less than a predetermined interval;

(3) in response to determining that the synchronization request was received in less than a predetermined interval ignoring the synchronization request; and

(4) in response to determining that the synchronization request was not received in less than a predetermined interval, providing the response to the first computer.

65. The computer of claim 64, wherein the computer delays the acceptance of a SYNC_REQ in step (3) for W/R seconds, where W is the number of data packets between synchronization requests according to an agreed schedule, and R is the agreed rate at which synchronization requests should be received according to the agreed schedule.

66. The computer of claim 64, wherein the computer further performs the step of determining whether the synchronization request is a duplicate of a previously received synchronization request and, if it is a duplicate, discarding it.

67. A method of establishing communication between one of a plurality of client computers and a central computer that maintains a plurality of authentication tables each corresponding to one of the client computers, the method comprising the steps of:

(1) in the central computer, receiving from one of the plurality of client computers a request to establish a connection;

(2) authenticating, with reference to one of the plurality of authentication tables, that the request received in step (1) is from an authorized client;

(3) responsive to a determination that the request is from an authorized client, allocating resources to establish a virtual private link between the client and a second computer; and

(4) communicating between the authorized client and the second computer using the virtual private link.

68. The method of claim 67, wherein step (4) comprises the step of communicating according to a scheme by which at least one field in a series of data packets is periodically changed according to a known sequence.

69. The method of claim 68, wherein step (4) comprises the step of comparing an Internet Protocol (IP) address in a header of each data packet to a table of valid IP addresses maintained in a table in the second computer.

70. The method of claim 69, wherein step (4) comprises the step of comparing the IP address in the header of each data packet to a moving window of valid IP addresses, and rejecting data packets having IP addresses that do not fall within the moving window.

71. The method of claim 67, wherein step (2) comprises the step of using a checkpoint data structure that maintains synchronization of a periodically changing parameter known by the central computer and the client computer to authenticate the client.

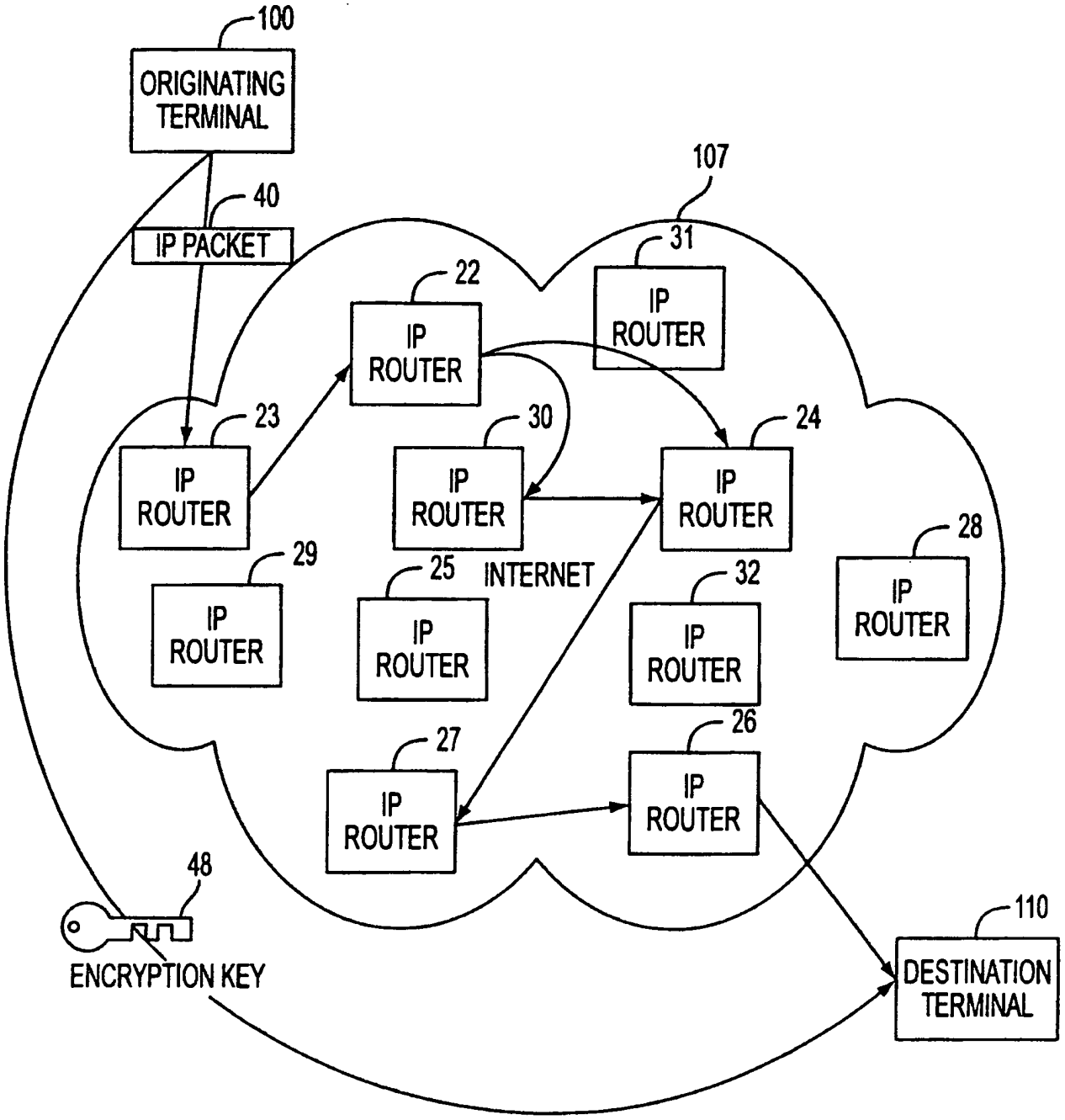

100
ORIGINATING TERMINAL
40
IP PACKET
107
31
IP ROUTER
22
IP ROUTER
23
IP ROUTER
30
IP ROUTER
24
IP ROUTER
29
IP ROUTER
25
IP ROUTER
INTERNET
32
IP ROUTER
28
IP ROUTER
27
IP ROUTER
26
IP ROUTER
48
ENCRYPTION KEY
110
DESTINATION TERMINAL

FIG. 1

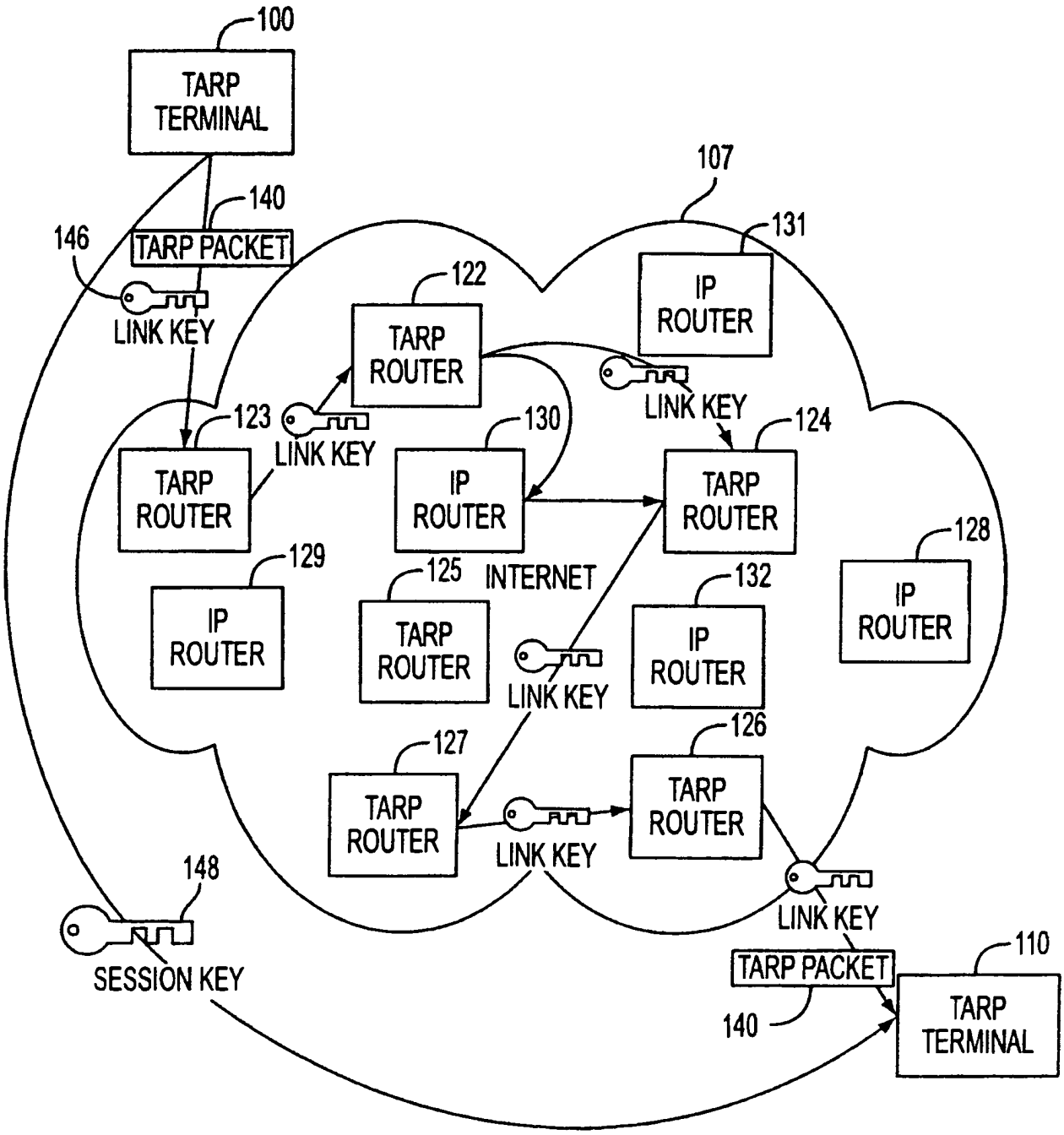

100
TARP TERMINAL
140
TARP PACKET
146
LINK KEY
107
131
IP ROUTER
122
TARP ROUTER
LINK KEY
123
LINK KEY
130
124
TARP ROUTER
IP ROUTER
TARP ROUTER
128
129
125
INTERNET
132
IP ROUTER
TARP ROUTER
IP ROUTER
IP ROUTER
LINK KEY
127
126
TARP ROUTER
LINK KEY
TARP ROUTER
148
LINK KEY
SESSION KEY
110
TARP PACKET
140
TARP TERMINAL

FIG. 2

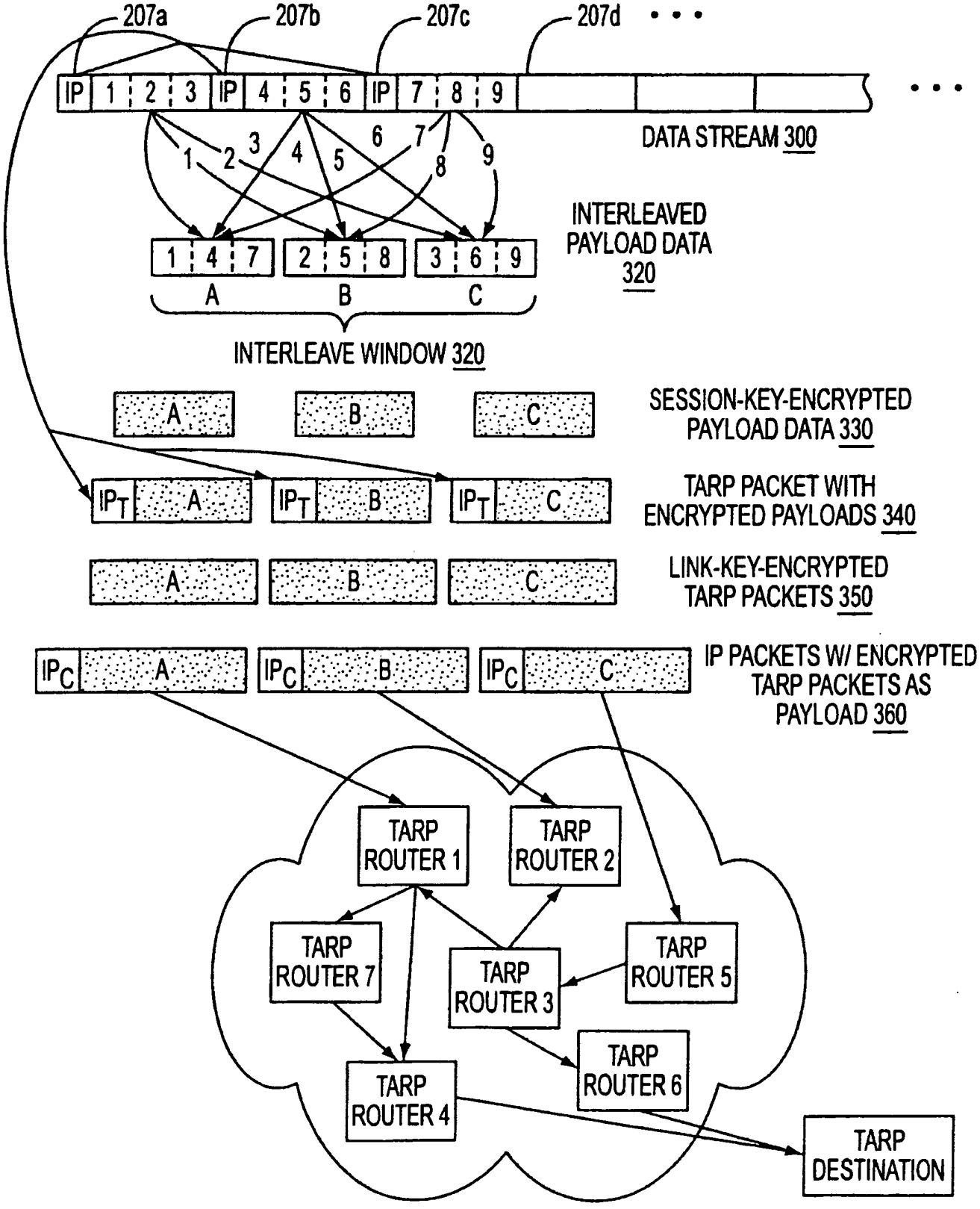

207a
207b
207c
207d
IP 1 2 3 IP 4 5 6 IP 7 8 9
DATA STREAM 300
1 2 3 4 5 6 7 8 9
1 4 7
2 5 8
3 6 9
A
B
C
INTERLEAVED PAYLOAD DATA 320
INTERLEAVE WINDOW 320
SESSION-KEY-ENCRYPTED PAYLOAD DATA 330
IPT A IPT B IPT C
TARP PACKET WITH ENCRYPTED PAYLOADS 340
LINK-KEY-ENCRYPTED TARP PACKETS 350
IPC A IPC B IPC C
IP PACKETS W/ ENCRYPTED TARP PACKETS AS PAYLOAD 360
TARP ROUTER 1
TARP ROUTER 2
TARP ROUTER 7
TARP ROUTER 3
TARP ROUTER 5
TARP ROUTER 6
TARP ROUTER 4
TARP DESTINATION

FIG. 3A

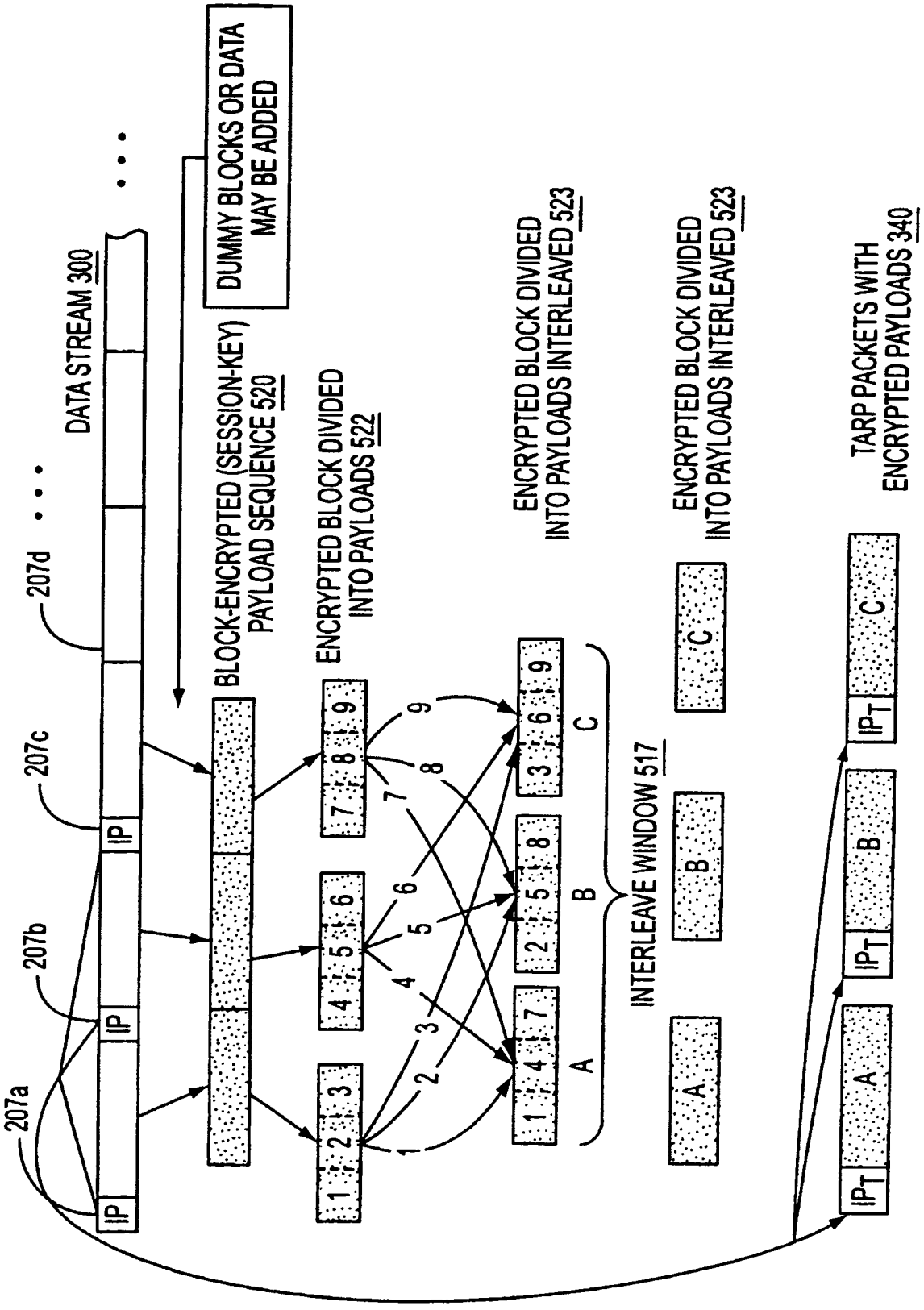

DATA STREAM 300
DUMMY BLOCKS OR DATA MAY BE ADDED
BLOCK-ENCRYPTED (SESSION-KEY) PAYLOAD SEQUENCE 520
ENCRYPTED BLOCK DIVIDED INTO PAYLOADS 522
ENCRYPTED BLOCK DIVIDED INTO PAYLOADS INTERLEAVED 523
INTERLEAVE WINDOW 517
TARP PACKETS WITH ENCRYPTED PAYLOADS 340
207a
207b
207c
207d
IP
IPT
A
B
C

FIG. 3B

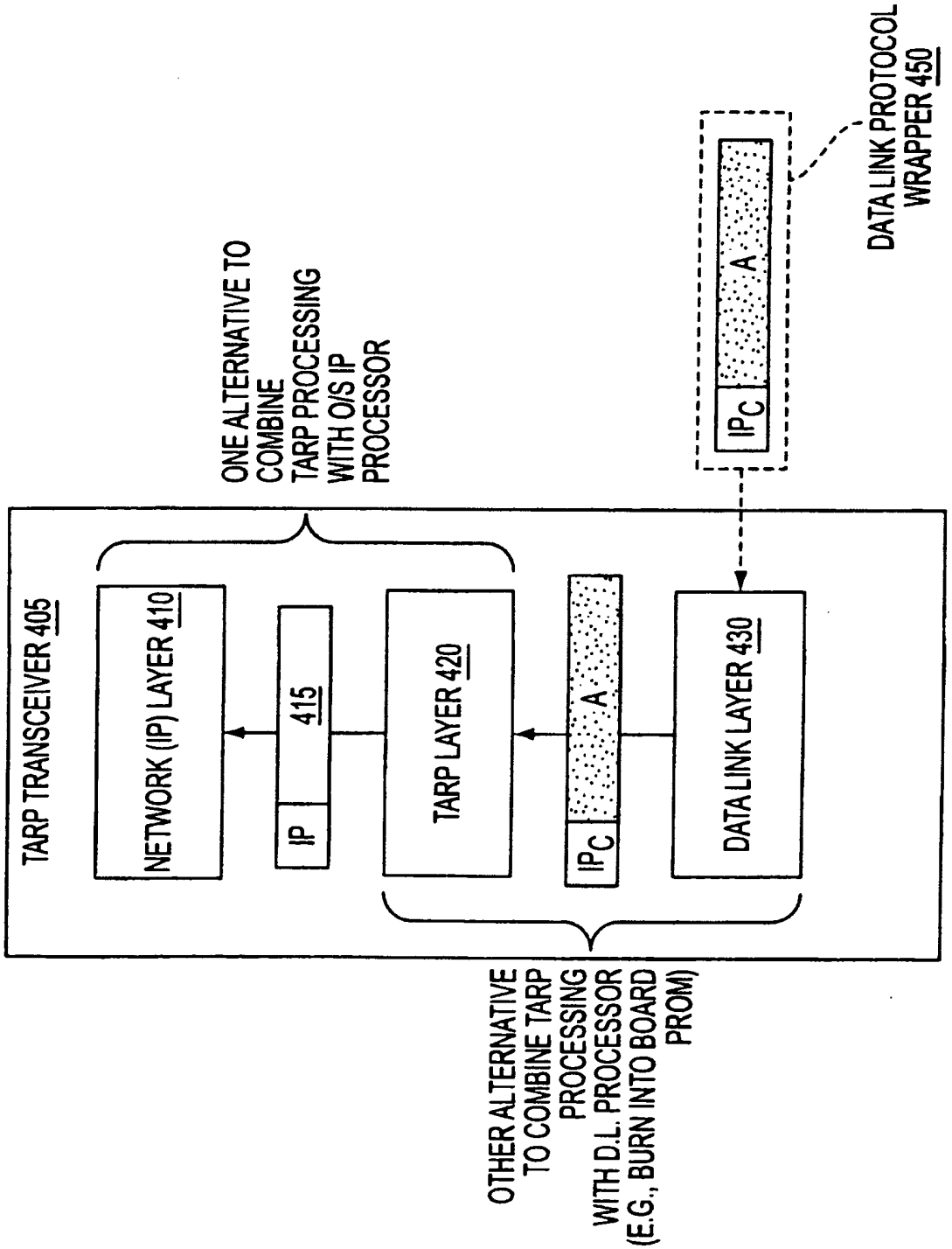
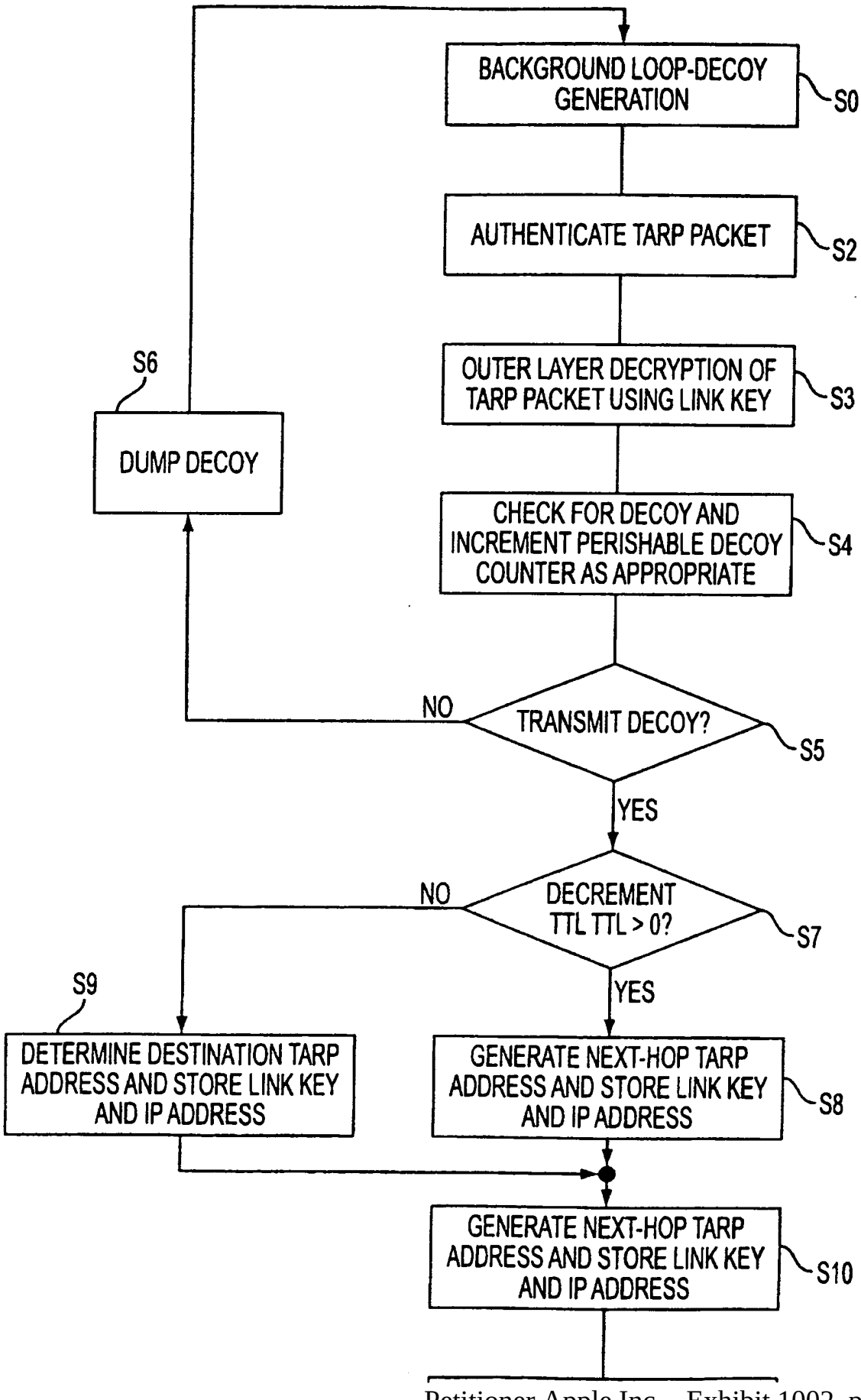

TARP TRANSCEIVER 405
NETWORK (IP) LAYER 410
IP
415
TARP LAYER 420
IPC
A
DATA LINK LAYER 430
ONE ALTERNATIVE TO COMBINE TARP PROCESSING WITH O/S IP PROCESSOR
OTHER ALTERNATIVE TO COMBINE TARP PROCESSING WITH D.L. PROCESSOR (E.G., BURN INTO BOARD PROM)
IPC
A
DATA LINK PROTOCOL WRAPPER 450

FIG. 4


BACKGROUND LOOP-DECOY GENERATION
S0
AUTHENTICATE TARP PACKET
S2
OUTER LAYER DECRYPTION OF TARP PACKET USING LINK KEY
S3
CHECK FOR DECOY AND INCREMENT PERISHABLE DECOY COUNTER AS APPROPRIATE
S4
TRANSMIT DECOY?
S5
NO
YES
S6
DUMP DECOY
DECREMENT TTL TTL > 0?
S7
NO
YES
S8
GENERATE NEXT-HOP TARP ADDRESS AND STORE LINK KEY AND IP ADDRESS
S9
DETERMINE DESTINATION TARP ADDRESS AND STORE LINK KEY AND IP ADDRESS
S10
GENERATE NEXT-HOP TARP ADDRESS AND STORE LINK KEY AND IP ADDRESS

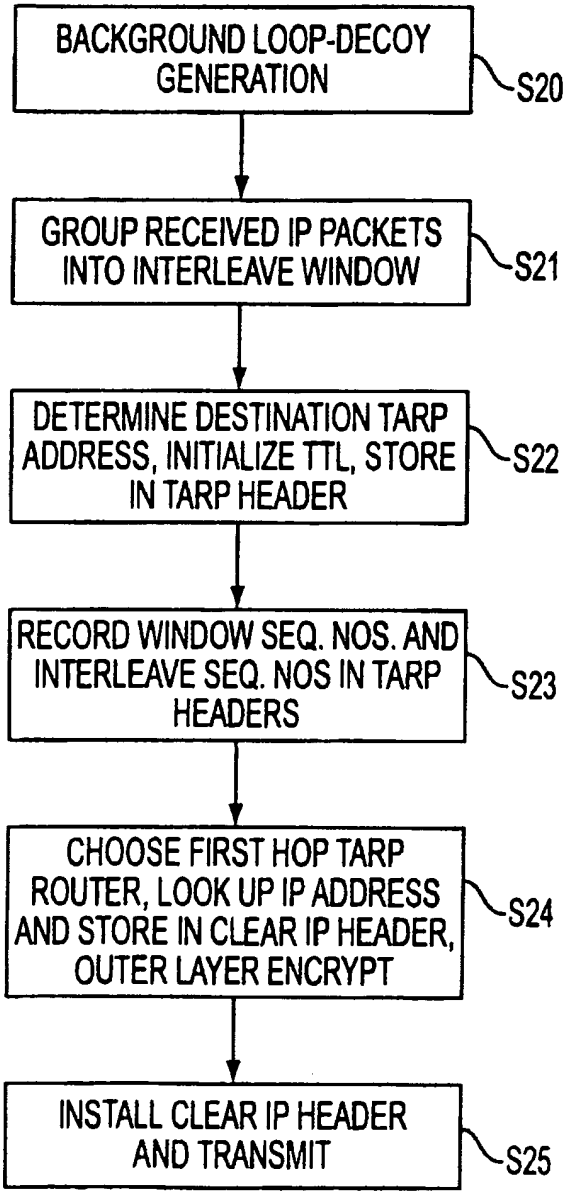

BACKGROUND LOOP-DECOY GENERATION
S20
GROUP RECEIVED IP PACKETS INTO INTERLEAVE WINDOW
S21
DETERMINE DESTINATION TARP ADDRESS, INITIALIZE TTL, STORE IN TARP HEADER
S22
RECORD WINDOW SEQ. NOS. AND INTERLEAVE SEQ. NOS IN TARP HEADERS
S23
CHOOSE FIRST HOP TARP ROUTER, LOOK UP IP ADDRESS AND STORE IN CLEAR IP HEADER, OUTER LAYER ENCRYPT
S24
INSTALL CLEAR IP HEADER AND TRANSMIT
S25

FIG. 6

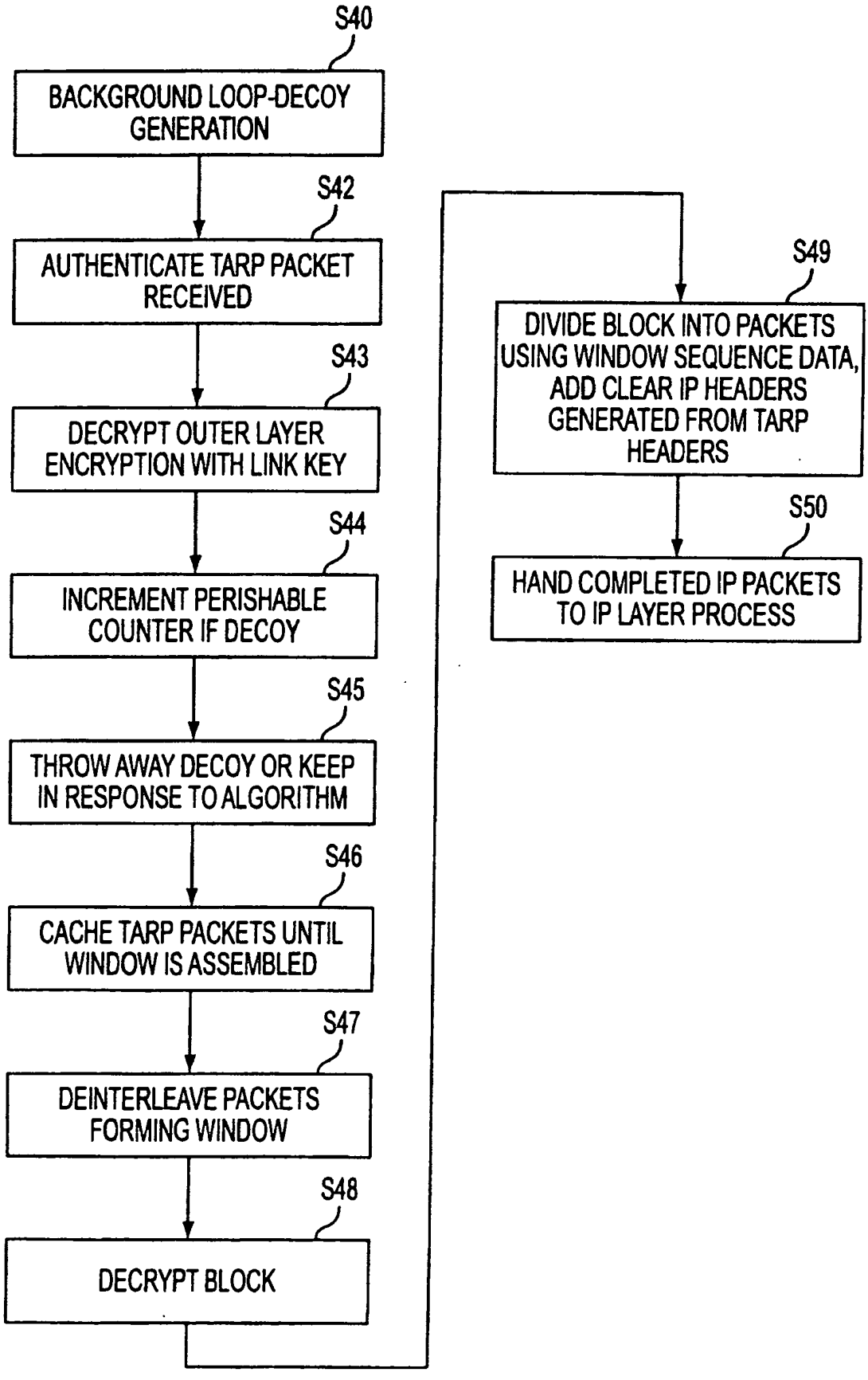

S40
BACKGROUND LOOP-DECOY GENERATION
S42
AUTHENTICATE TARP PACKET RECEIVED
S43
DECRYPT OUTER LAYER ENCRYPTION WITH LINK KEY
S44
INCREMENT PERISHABLE COUNTER IF DECOY
S45
THROW AWAY DECOY OR KEEP IN RESPONSE TO ALGORITHM
S46
CACHE TARP PACKETS UNTIL WINDOW IS ASSEMBLED
S47
DEINTERLEAVE PACKETS FORMING WINDOW
S48
DECRYPT BLOCK
S49
DIVIDE BLOCK INTO PACKETS USING WINDOW SEQUENCE DATA, ADD CLEAR IP HEADERS GENERATED FROM TARP HEADERS
S50
HAND COMPLETED IP PACKETS TO IP LAYER PROCESS

FIG. 7

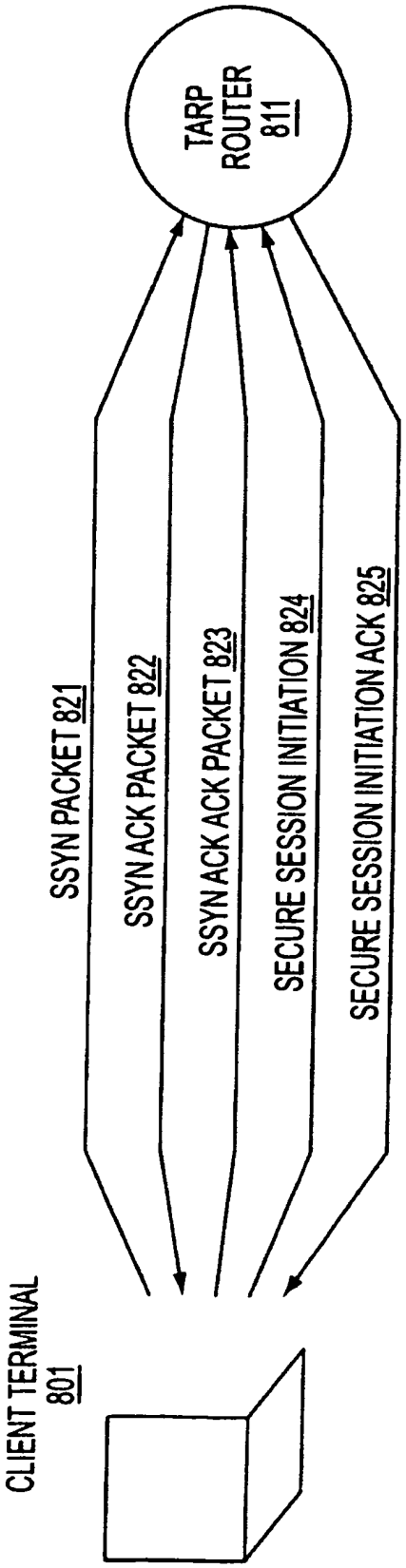

TARP ROUTER 811
SSYN PACKET 821
SSYN ACK PACKET 822
SSYN ACK ACK PACKET 823
SECURE SESSION INITIATION 824
SECURE SESSION INITIATION ACK 825
CLIENT TERMINAL 801

FIG. 8

CLIENT 1
901
TARP
ROUTER
911
TRANSMIT TABLE 921
131.218.204.98 , 131.218.204.65
131.218.204.221 , 131.218.204.97
131.218.204.139 , 131.218.204.186
131.218.204.12 , 131.218.204.55
RECEIVE TABLE 924
131.218.204.98 , 131.218.204.65
131.218.204.221 , 131.218.204.97
131.218.204.139 , 131.218.204.186
131.218.204.12 , 131.218.204.55
RECEIVE TABLE 922
131.218.204.161 , 131.218.204.89
131.218.204.66 , 131.218.204.212
131.218.204.201 , 131.218.204.127
131.218.204.119 , 131.218.204.49
TRANSMIT TABLE 923
131.218.204.161 , 131.218.204.89
131.218.204.66 , 131.218.204.212
131.218.204.201 , 131.218.204.127
131.218.204.119 , 131.218.204.49

FIG. 9

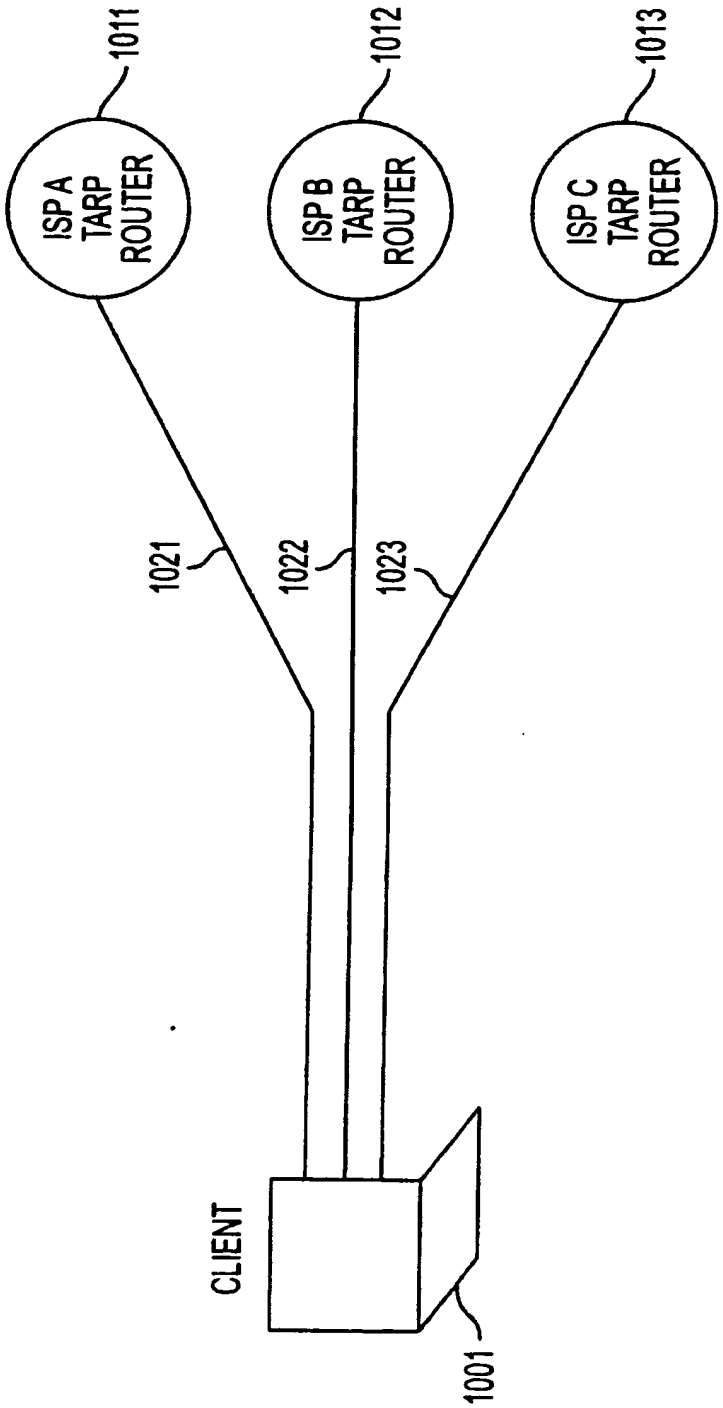

1011
1012
1013
ISP A TARP ROUTER
ISP B TARP ROUTER
ISP C TARP ROUTER
1021
1022
1023
CLIENT
1001

FIG. 10

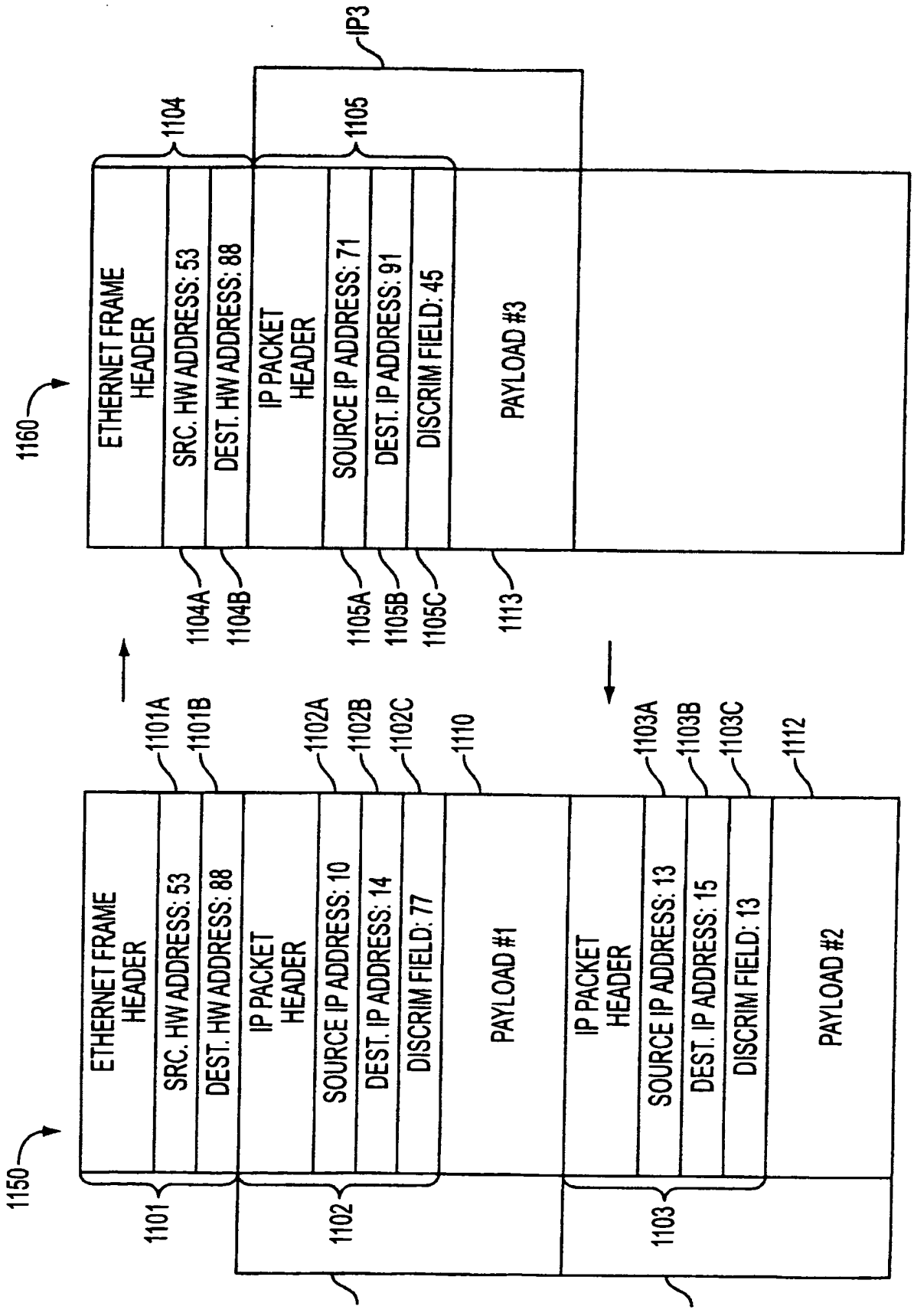

1150
1160
ETHERNET FRAME HEADER
SRC. HW ADDRESS: 53
DEST. HW ADDRESS: 88
IP PACKET HEADER
SOURCE IP ADDRESS: 10
DEST. IP ADDRESS: 14
DISCRIM FIELD: 77
PAYLOAD #1
IP PACKET HEADER
SOURCE IP ADDRESS: 13
DEST. IP ADDRESS: 15
DISCRIM FIELD: 13
PAYLOAD #2
ETHERNET FRAME HEADER
SRC. HW ADDRESS: 53
DEST. HW ADDRESS: 88
IP PACKET HEADER
SOURCE IP ADDRESS: 71
DEST. IP ADDRESS: 91
DISCRIM FIELD: 45
PAYLOAD #3
IP3
1101
1102
1103
1104
1105
1101A
1101B
1102A
1102B
1102C
1103A
1103B
1103C
1104A
1104B
1105A
1105B
1105C
1110
1112
1113

FIG. 11

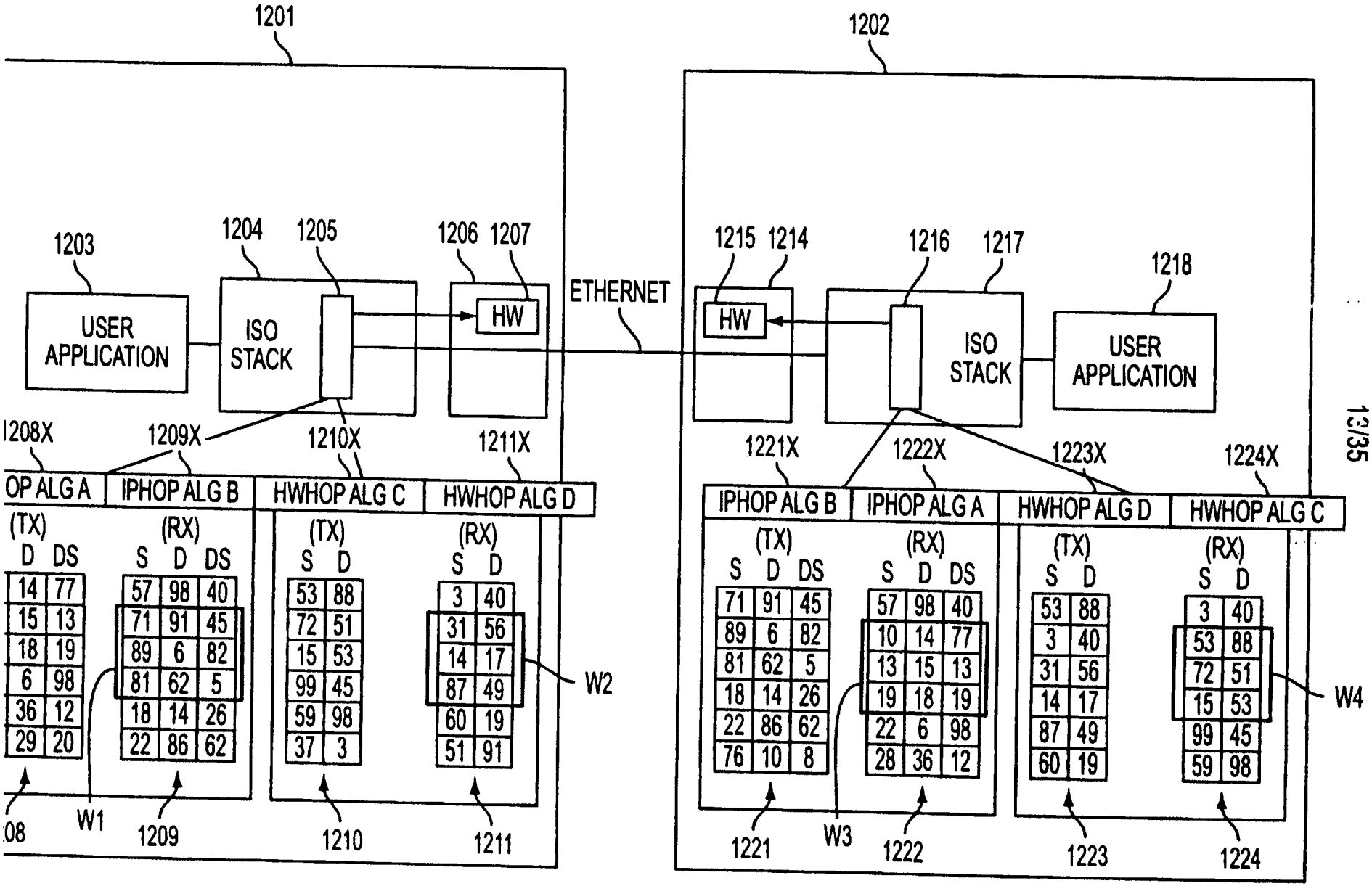


FIG. 12A

Petitioner Apple Inc. - Exhibit 1002, p. 1062

MODE OR EMBODIMENT	HARDWARE ADDRESSES	IP ADDRESSES	DISCRIMINATOR FIELD VALUES
1. PROMISCUOUS	SAME FOR ALL NODES OR COMPLETELY RANDOM	CAN BE VARIED IN SYNC	CAN BE VARIED IN SYNC
2. PROMISCUOUS PER VPN	FIXED FOR EACH VPN	CAN BE VARIED IN SYNC	CAN BE VARIED IN SYNC
3. HARDWARE HOPPING	CAN BE VARIED IN SYNC	CAN BE VARIED IN SYNC	CAN BE VARIED IN SYNC

FIG. 12B

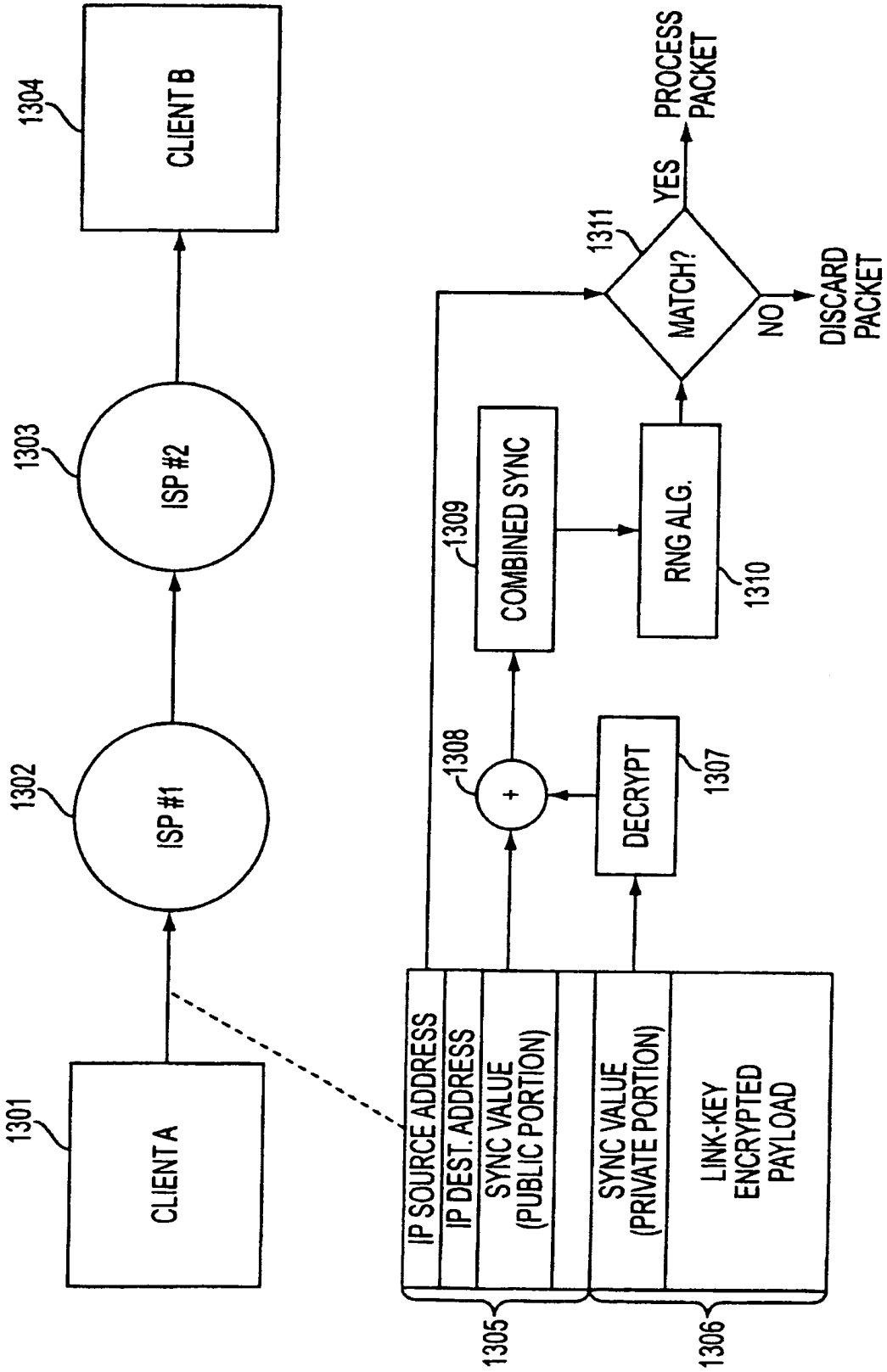

CLIENT A
1301
ISP #1
1302
ISP #2
1303
CLIENT B
1304
IP SOURCE ADDRESS
IP DEST. ADDRESS
SYNC VALUE (PUBLIC PORTION)
SYNC VALUE (PRIVATE PORTION)
LINK-KEY ENCRYPTED PAYLOAD
1305
1306
DECRYPT
1307
+
1308
COMBINED SYNC
1309
RNG ALG.
1310
MATCH?
1311
YES
PROCESS PACKET
NO
DISCARD PACKET

FIG. 13

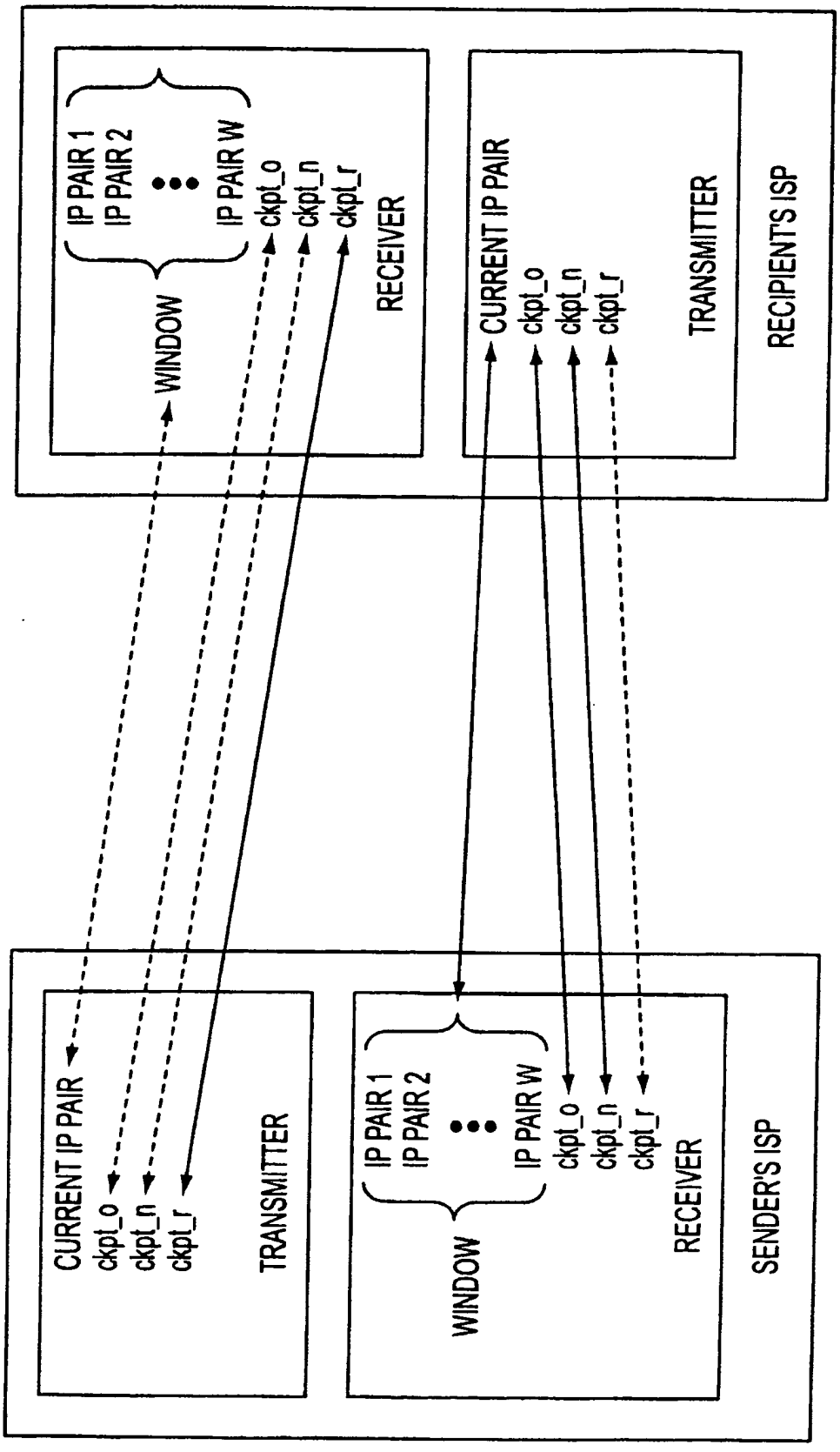

RECIPIENT'S ISP
TRANSMITTER
CURRENT IP PAIR
ckpt_o
ckpt_n
ckpt_r
RECEIVER
IP PAIR 1
IP PAIR 2
IP PAIR W
WINDOW
ckpt_o
ckpt_n
ckpt_r
SENDER'S ISP
TRANSMITTER
CURRENT IP PAIR
ckpt_o
ckpt_n
ckpt_r
RECEIVER
IP PAIR 1
IP PAIR 2
IP PAIR W
WINDOW
ckpt_o
ckpt_n
ckpt_r
KEPT IN SYNC FOR SENDER TO RECIPIENT SYNCHRONIZER
KEPT IN SYNC FOR RECIPIENT TO SENDER SYNCHRONIZER

FIG. 14

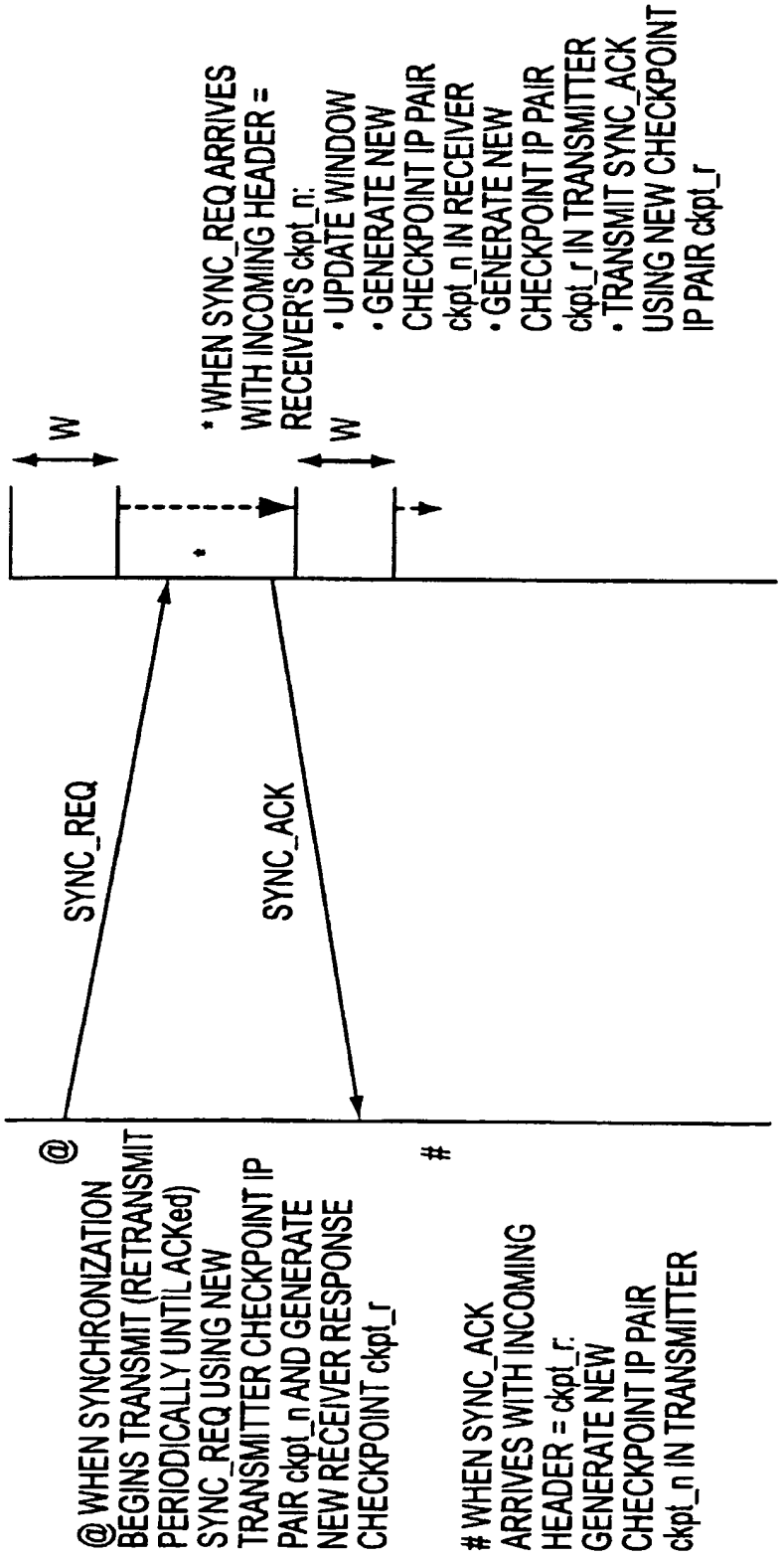

W
W
* WHEN SYNC_REQ ARRIVES WITH INCOMING HEADER = RECEIVER'S ckpt_n:
• UPDATE WINDOW
• GENERATE NEW CHECKPOINT IP PAIR ckpt_n IN RECEIVER
• GENERATE NEW CHECKPOINT IP PAIR ckpt_r IN TRANSMITTER
• TRANSMIT SYNC_ACK USING NEW CHECKPOINT IP PAIR ckpt_r
SYNC_REQ
SYNC_ACK
@
#
@ WHEN SYNCHRONIZATION BEGINS TRANSMIT (RETRANSMIT PERIODICALLY UNTIL ACKed) SYNC_REQ USING NEW TRANSMITTER CHECKPOINT IP PAIR ckpt_n AND GENERATE NEW RECEIVER RESPONSE CHECKPOINT ckpt_r
# WHEN SYNC_ACK ARRIVES WITH INCOMING HEADER = ckpt_r: GENERATE NEW CHECKPOINT IP PAIR ckpt_n IN TRANSMITTER

FIG. 15

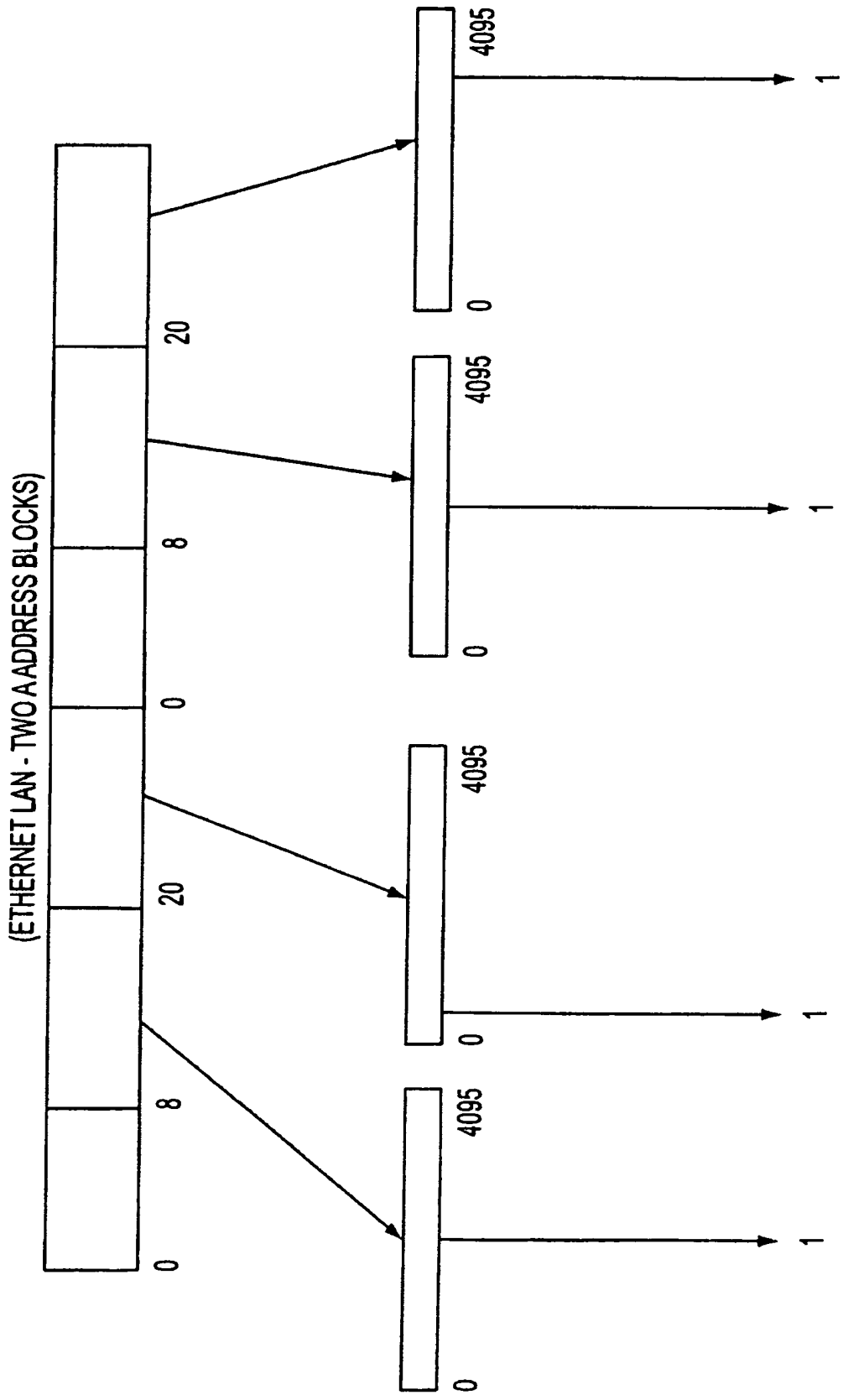

(ETHERNET LAN - TWO ADDRESS BLOCKS)
20
8
0
20
8
0
4095
0
1
4095
0
1
4095
0
1
4095
0
1

FIG. 16

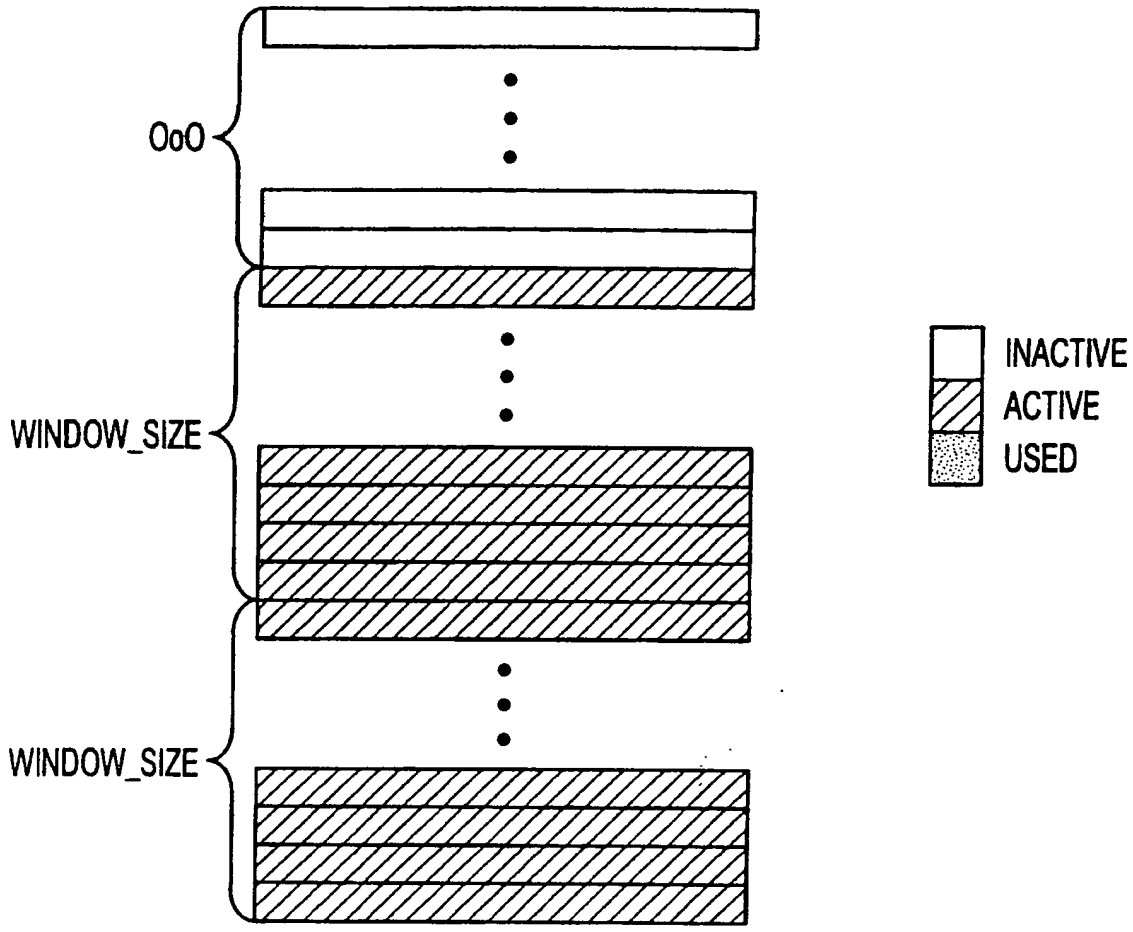


FIG. 17

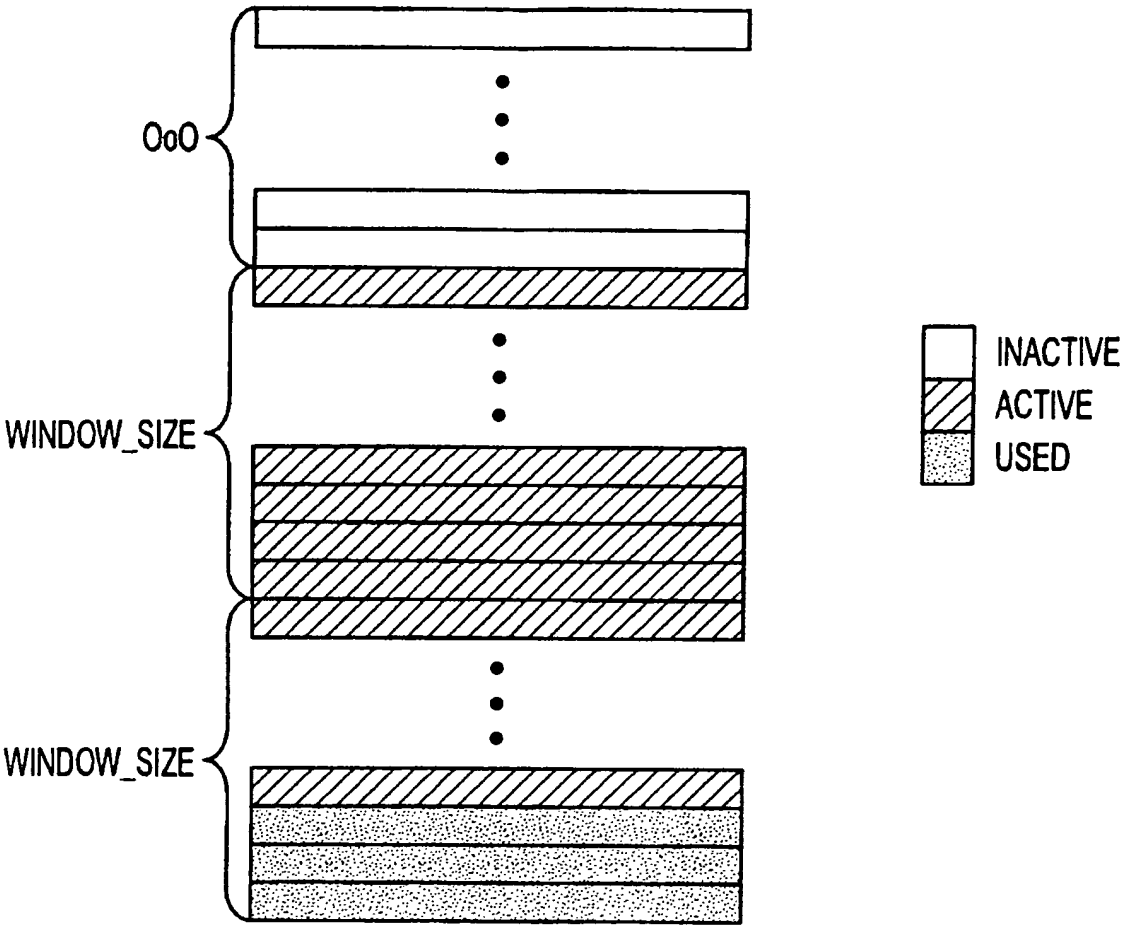


FIG. 18

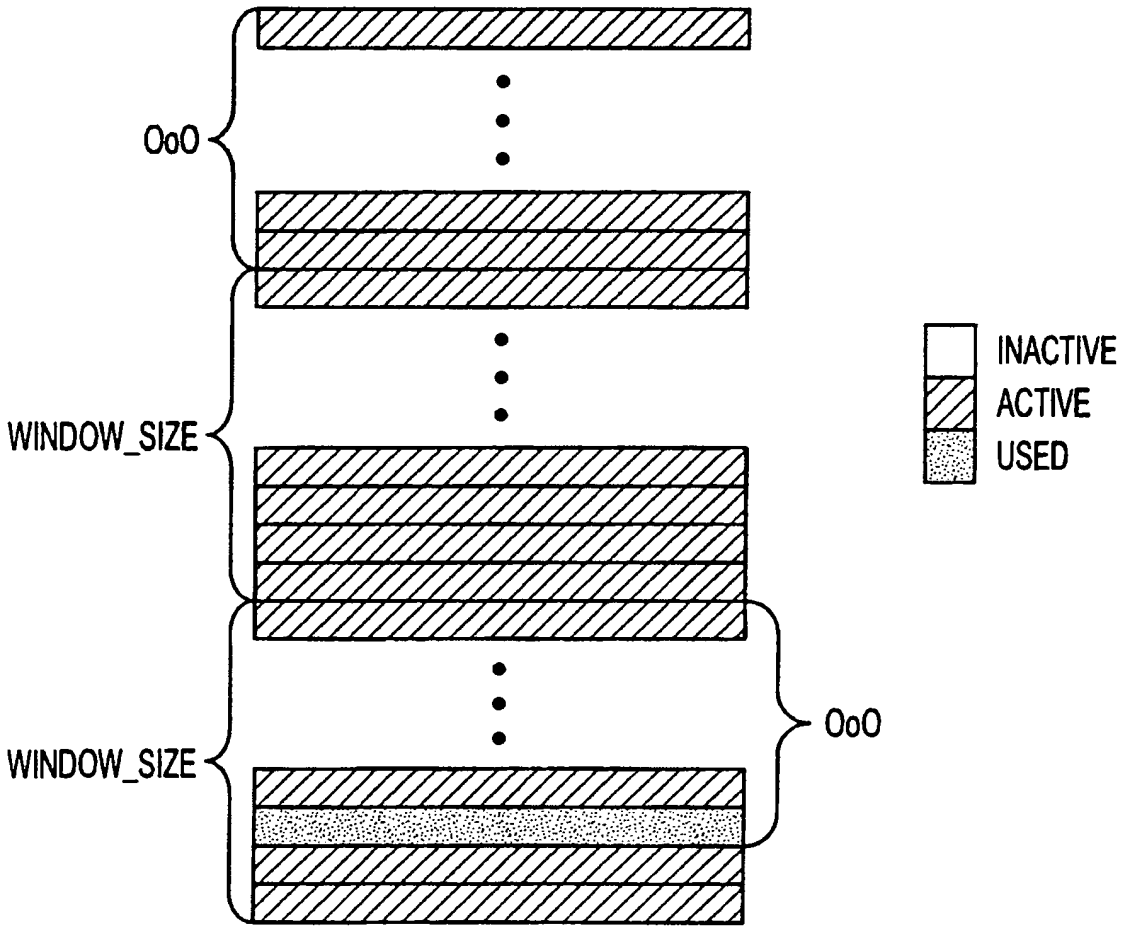


FIG. 19

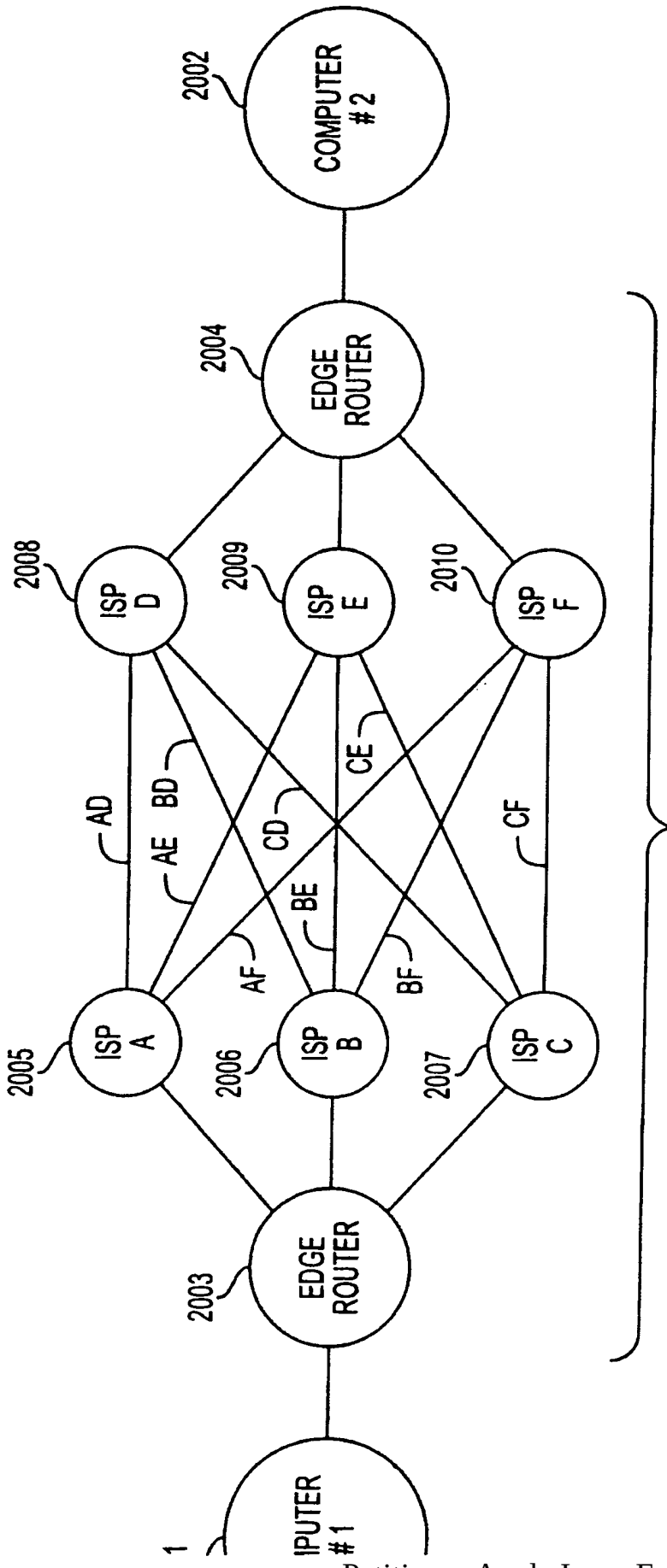
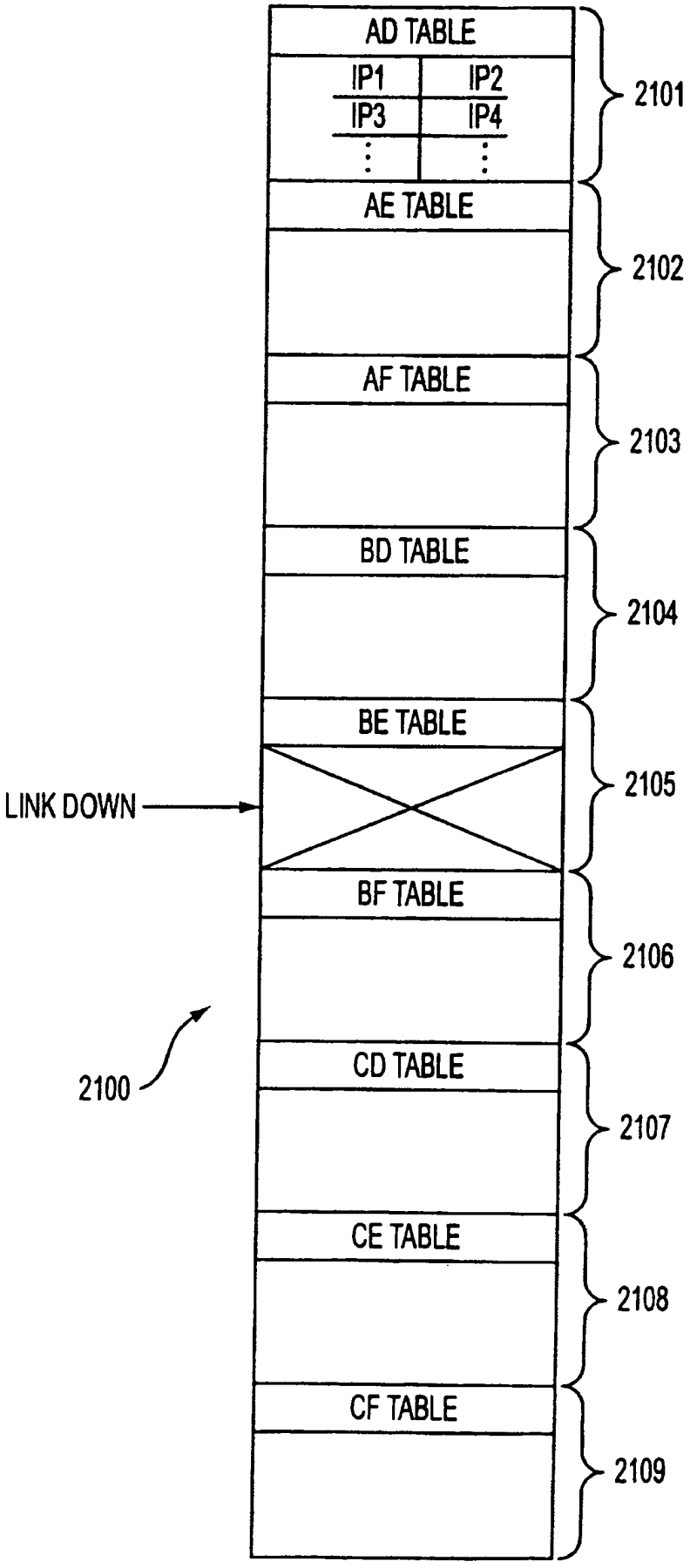
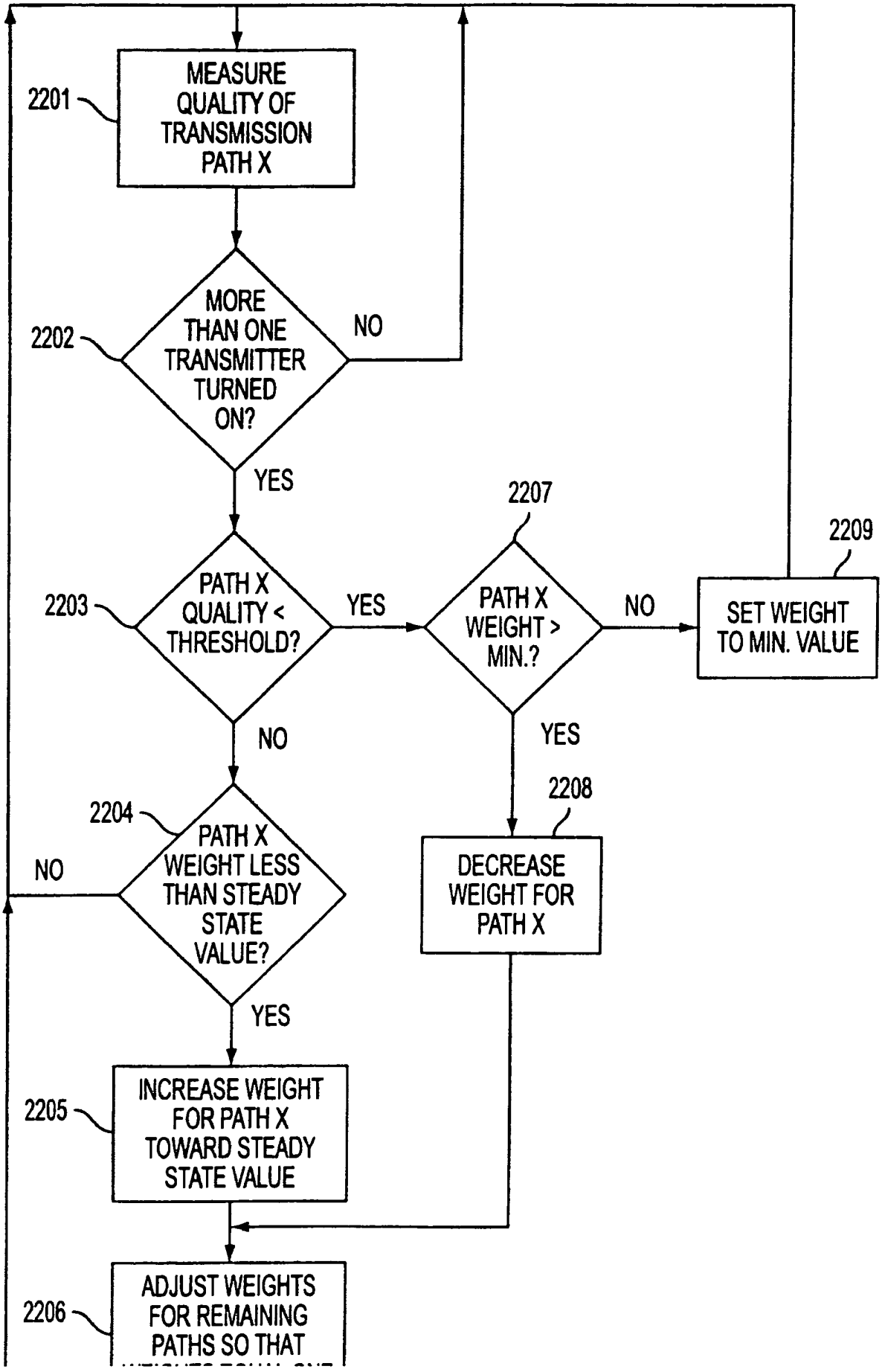

2002
COMPUTER #2
2004
EDGE ROUTER
2008
ISP D
2009
ISP E
2010
ISP F
AD
AE
BD
CD
CE
CF
AF
BE
BF
2005
ISP A
2006
ISP B
2007
ISP C
2003
EDGE ROUTER
1
IPUTER #1
2011

FIG. 20


AD TABLE
IP1
IP2
IP3
IP4
2101
AE TABLE
2102
AF TABLE
2103
BD TABLE
2104
BE TABLE
LINK DOWN
2105
BF TABLE
2106
2100
CD TABLE
2107
CE TABLE
2108
CF TABLE
2109


MEASURE QUALITY OF TRANSMISSION PATH X
2201
MORE THAN ONE TRANSMITTER TURNED ON?
2202
NO
YES
PATH X QUALITY < THRESHOLD?
2203
YES
NO
2207
PATH X WEIGHT > MIN.?
NO
YES
2209
SET WEIGHT TO MIN. VALUE
2208
DECREASE WEIGHT FOR PATH X
2204
PATH X WEIGHT LESS THAN STEADY STATE VALUE?
NO
YES
INCREASE WEIGHT FOR PATH X TOWARD STEADY STATE VALUE
2205
ADJUST WEIGHTS FOR REMAINING PATHS SO THAT
2206

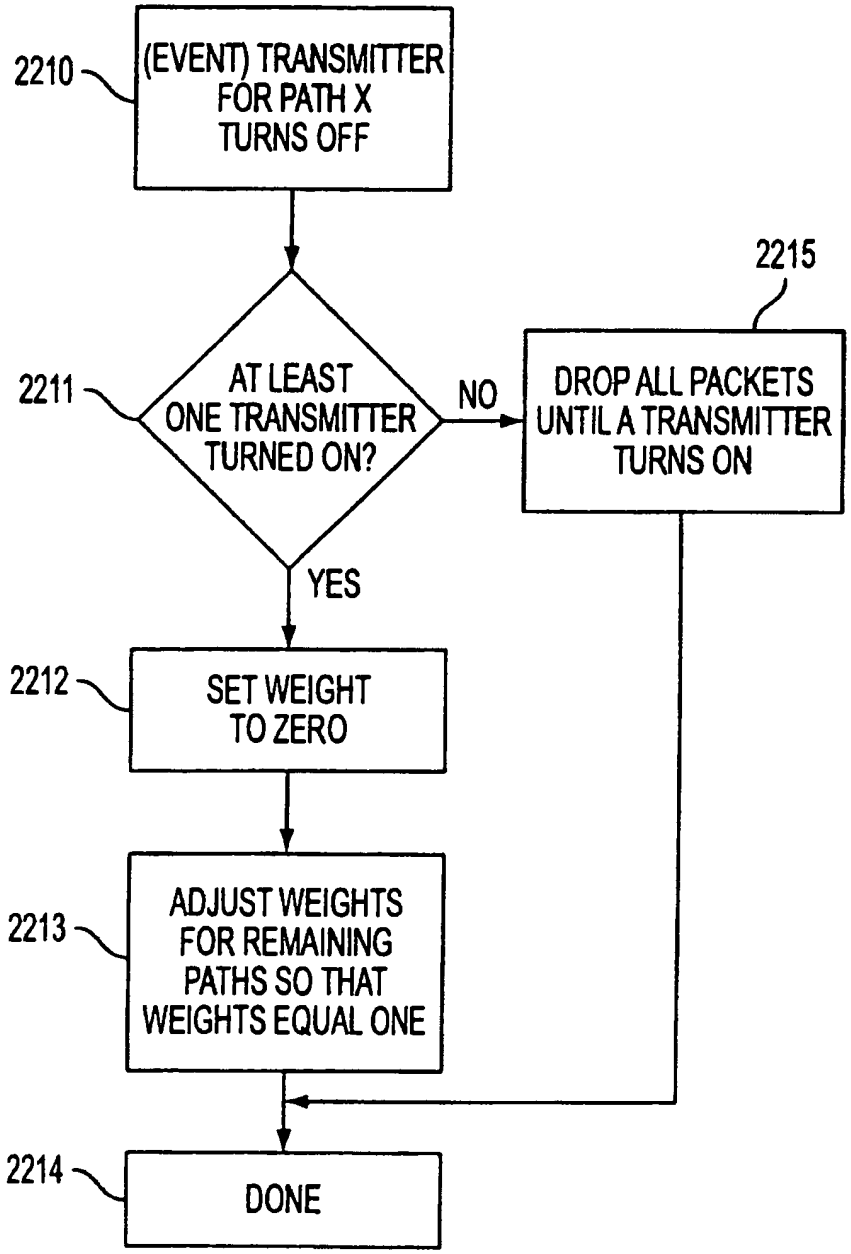

2210
(EVENT) TRANSMITTER FOR PATH X TURNS OFF
2211
AT LEAST ONE TRANSMITTER TURNED ON?
NO
2215
DROP ALL PACKETS UNTIL A TRANSMITTER TURNS ON
YES
2212
SET WEIGHT TO ZERO
2213
ADJUST WEIGHTS FOR REMAINING PATHS SO THAT WEIGHTS EQUAL ONE
2214
DONE

FIG. 22B

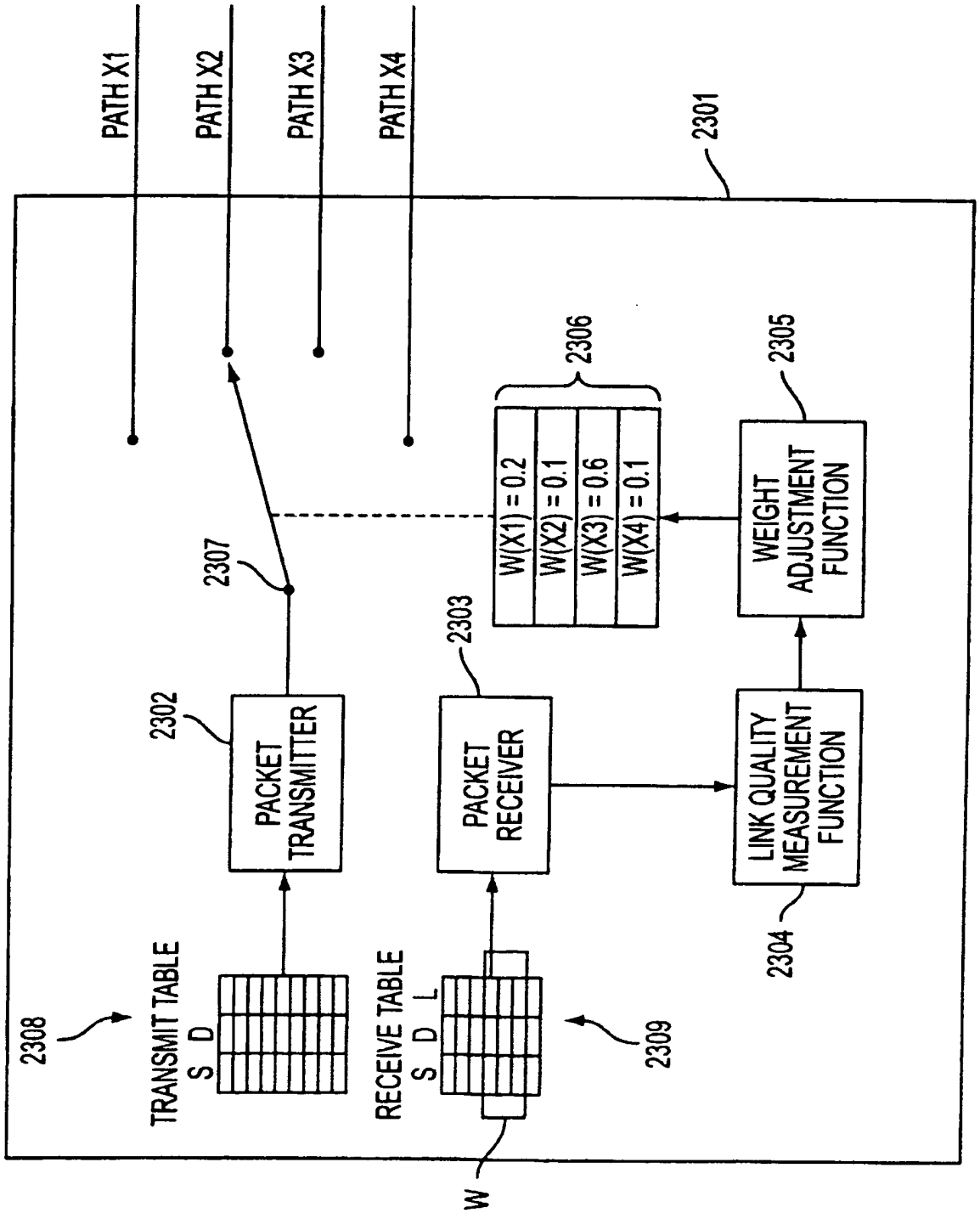

PATH X1
PATH X2
PATH X3
PATH X4
2301
2306
2305
W(X1) = 0.2
W(X2) = 0.1
W(X3) = 0.6
W(X4) = 0.1
WEIGHT ADJUSTMENT FUNCTION
2307
2303
2302
PACKET TRANSMITTER
PACKET RECEIVER
LINK QUALITY MEASUREMENT FUNCTION
2304
2308
TRANSMIT TABLE
S D
RECEIVE TABLE
S D L
2309
W

FIG. 23

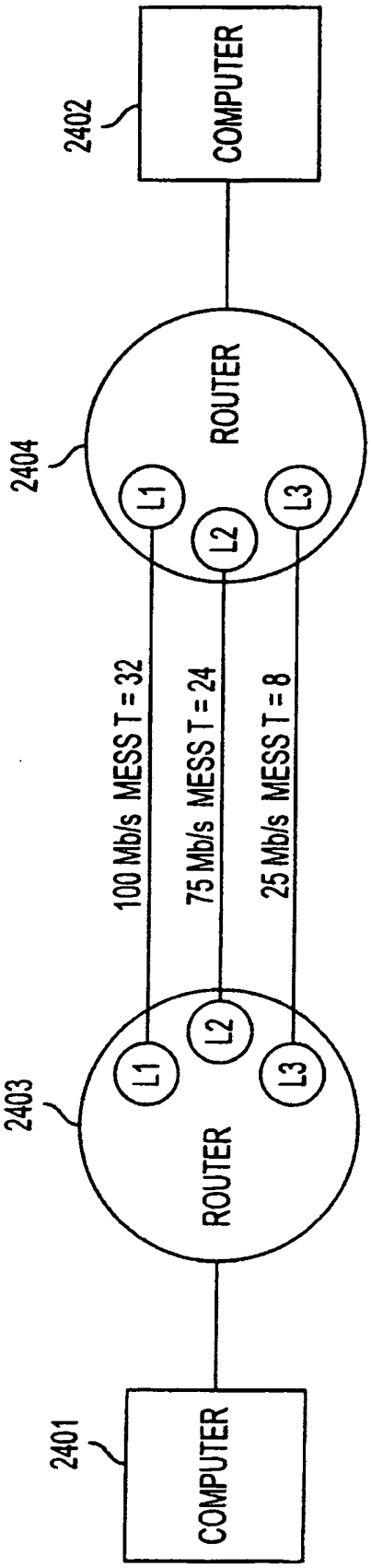

2402
COMPUTER
2404
ROUTER
L1
L2
L3
100 Mb/s MESS T = 32
75 Mb/s MESS T = 24
25 Mb/s MESS T = 8
2403
ROUTER
L1
L2
L3
2401
COMPUTER

FIG. 24

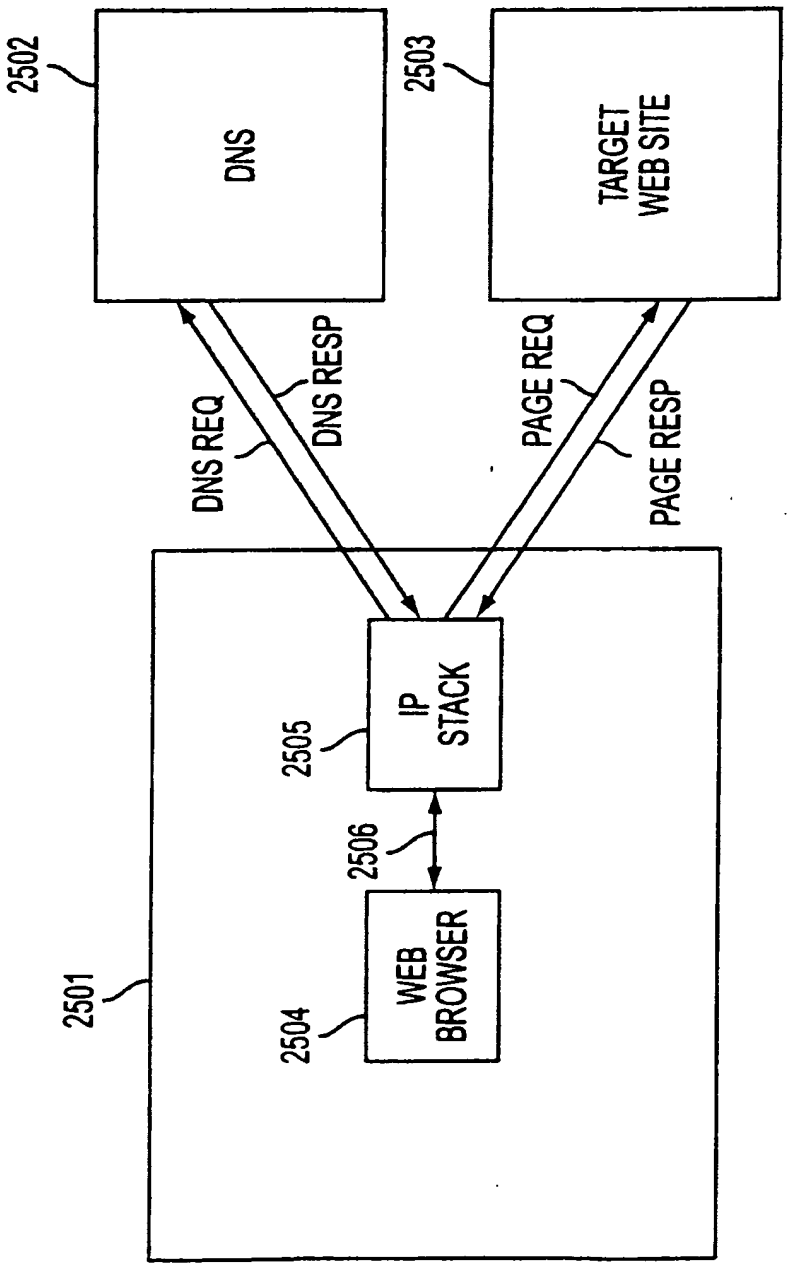


FIG. 25
(PRIOR ART)

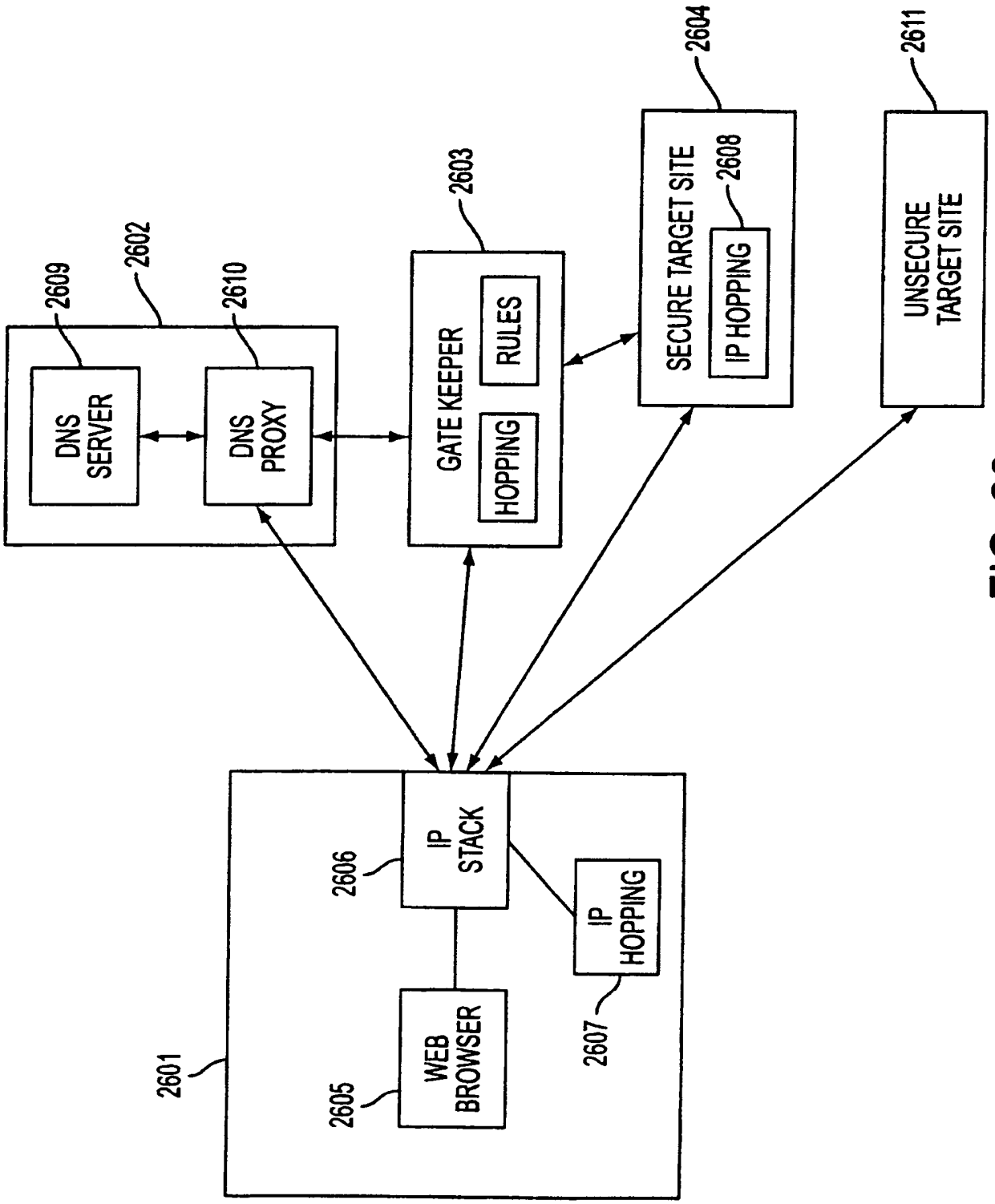

2601
2605
WEB BROWSER
2606
IP STACK
2607
IP HOPPING
2609
DNS SERVER
2602
2610
DNS PROXY
2603
GATE KEEPER
RULES
HOPPING
2604
SECURE TARGET SITE
2608
IP HOPPING
2611
UNSECURE TARGET SITE

FIG. 26

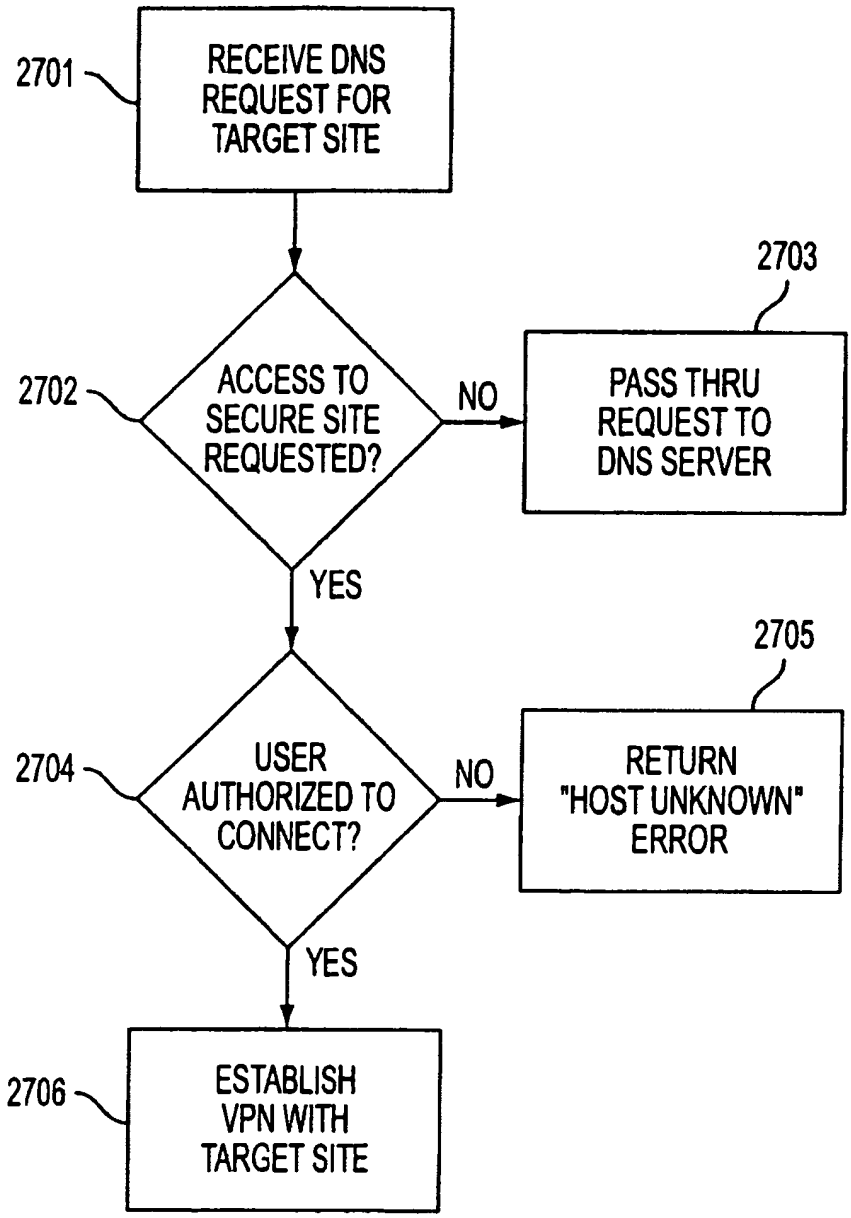

2701
RECEIVE DNS REQUEST FOR TARGET SITE
2702
ACCESS TO SECURE SITE REQUESTED?
NO
2703
PASS THRU REQUEST TO DNS SERVER
YES
2704
USER AUTHORIZED TO CONNECT?
NO
2705
RETURN "HOST UNKNOWN" ERROR
YES
2706
ESTABLISH VPN WITH TARGET SITE

FIG. 27

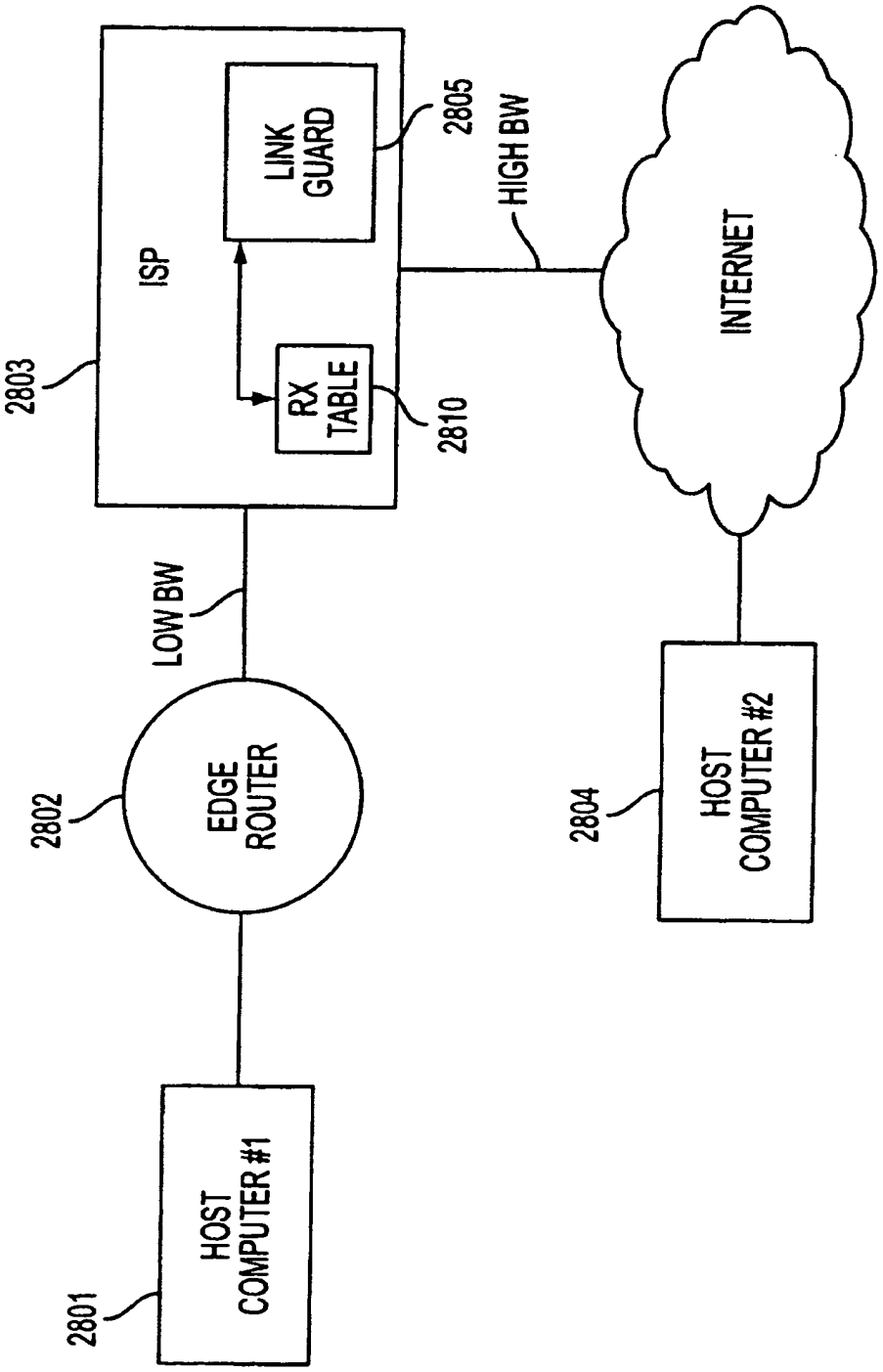

HOST COMPUTER #1
2801
EDGE ROUTER
2802
LOW BW
ISP
2803
LINK GUARD
2805
RX TABLE
2810
HIGH BW
INTERNET
HOST COMPUTER #2
2804

FIG. 28

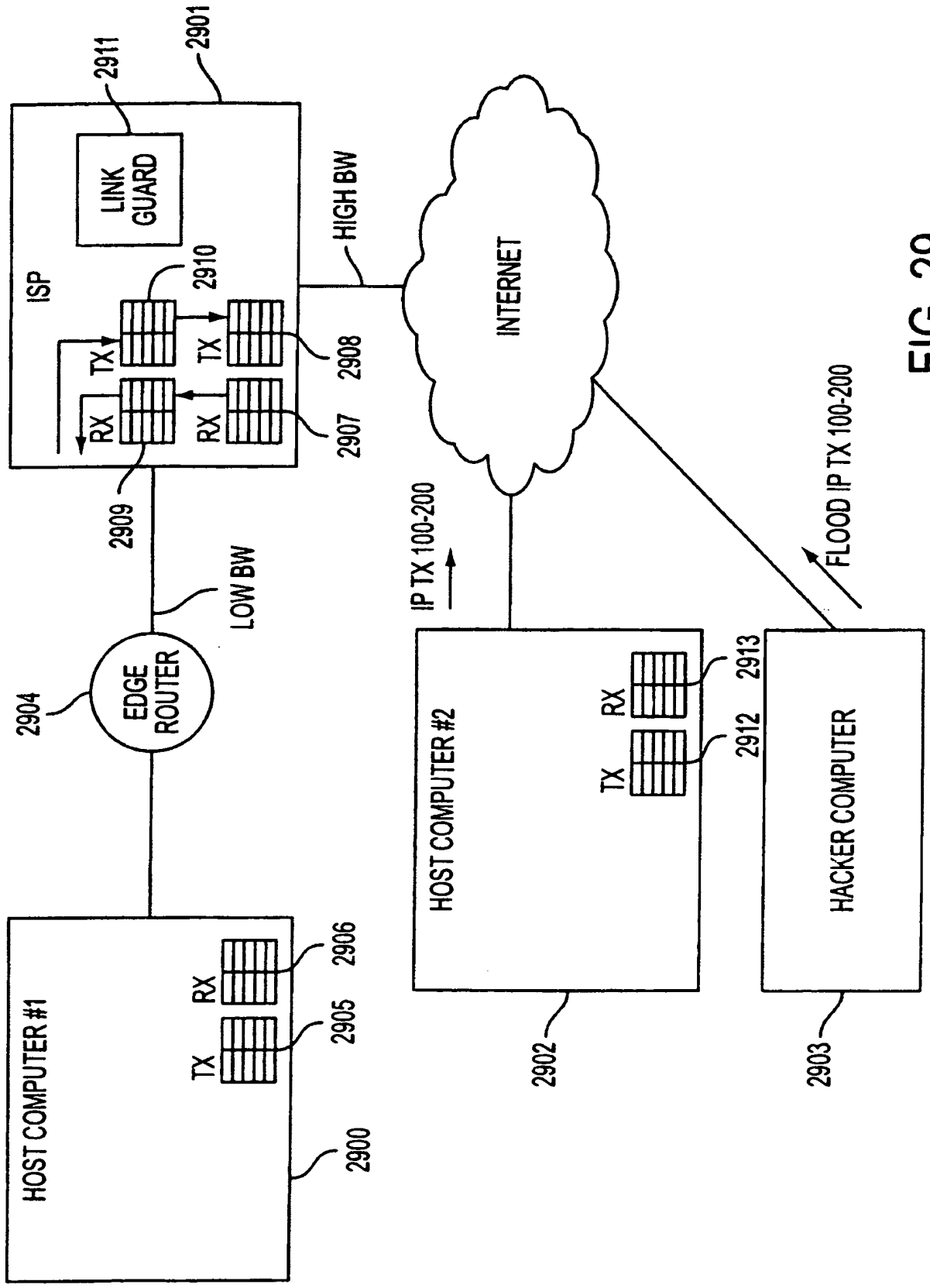

HOST COMPUTER #1
2900
TX
RX
2905
2906
2904
EDGE ROUTER
LOW BW
2909
ISP
2911
LINK GUARD
2901
HIGH BW
2910
TX
RX
TX
RX
2907
2908
INTERNET
IP TX 100-200
FLOOD IP TX 100-200
HOST COMPUTER #2
2902
TX
RX
2912
2913
HACKER COMPUTER
2903

FIG. 29

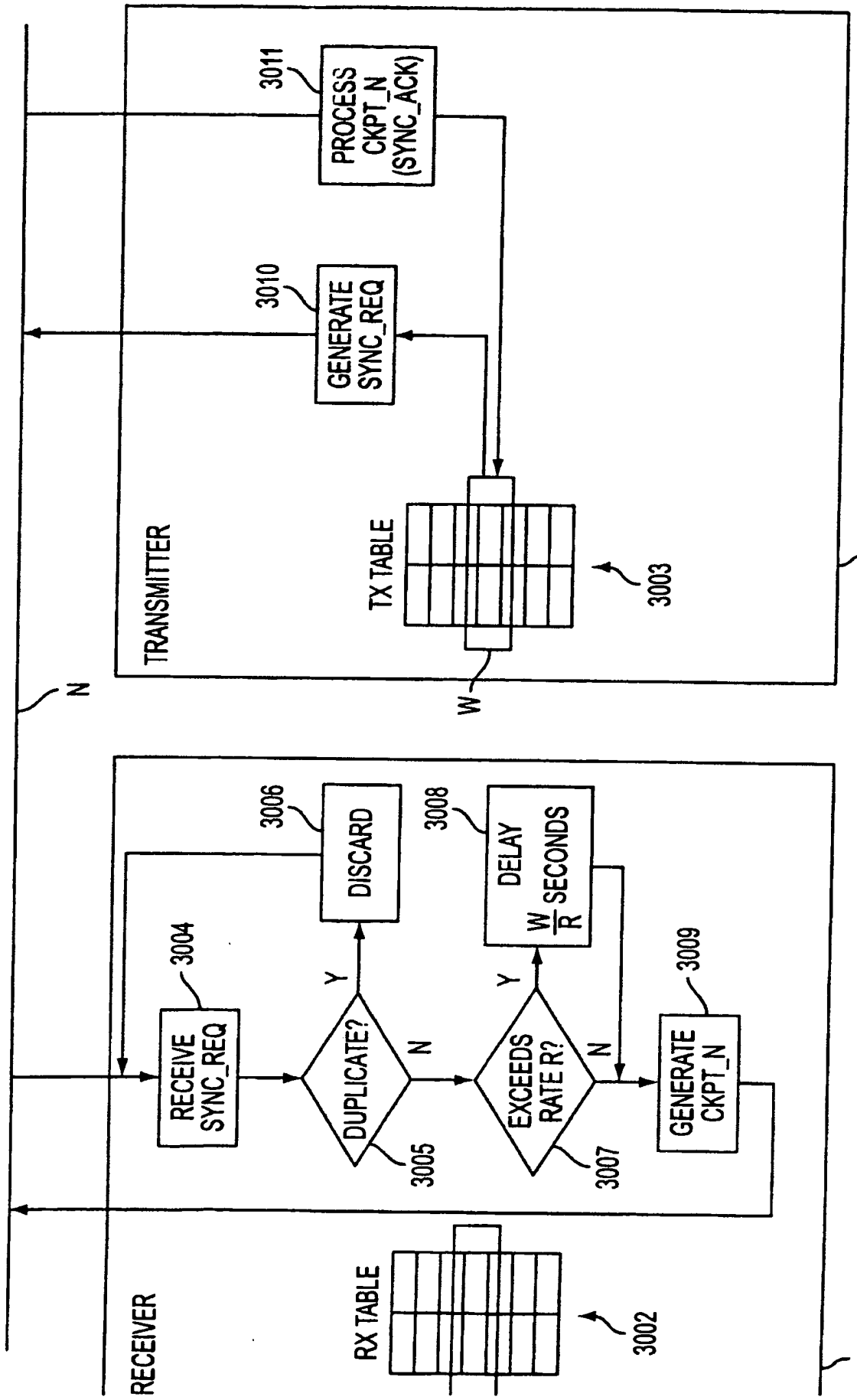

3011
PROCESS CKPT_N (SYNC_ACK)
3010
GENERATE SYNC_REQ
TRANSMITTER
TX TABLE
3003
3001
W
N
3006
DISCARD
3008
DELAY W/R SECONDS
3004
RECEIVE SYNC_REQ
Y
DUPLICATE?
N
3005
Y
EXCEEDS RATE R?
N
3007
3009
GENERATE CKPT_N
RECEIVER
RX TABLE
3002
3000

FIG. 30

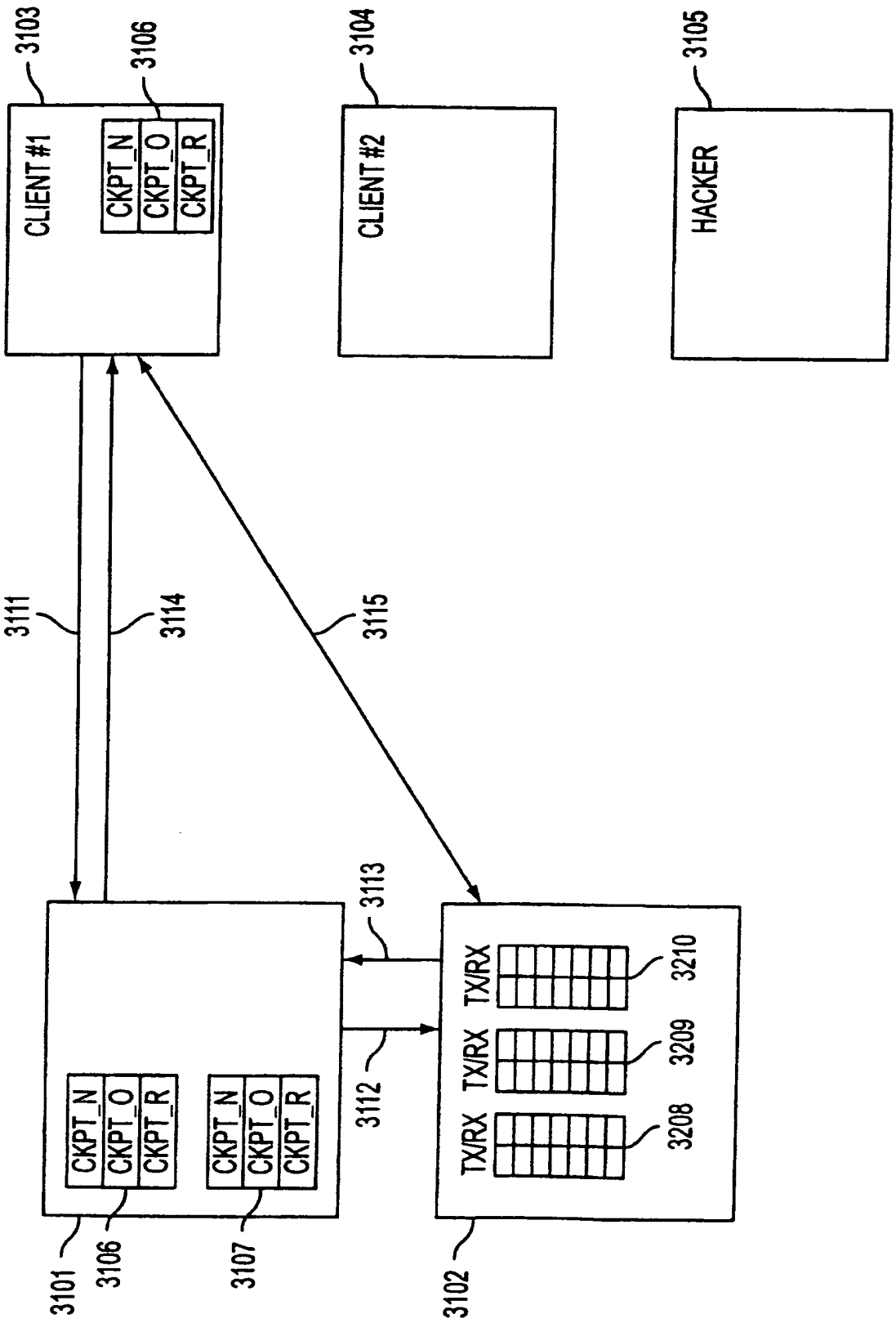

3103
3106
CLIENT #1
CKPT_N
CKPT_O
CKPT_R
3104
CLIENT #2
3105
HACKER
3111
3114
3115
3113
3112
3101
3106
3107
3102
CKPT_N
CKPT_O
CKPT_R
CKPT_N
CKPT_O
CKPT_R
TX/RX
TX/RX
TX/RX
3210
3209
3208

FIG. 31

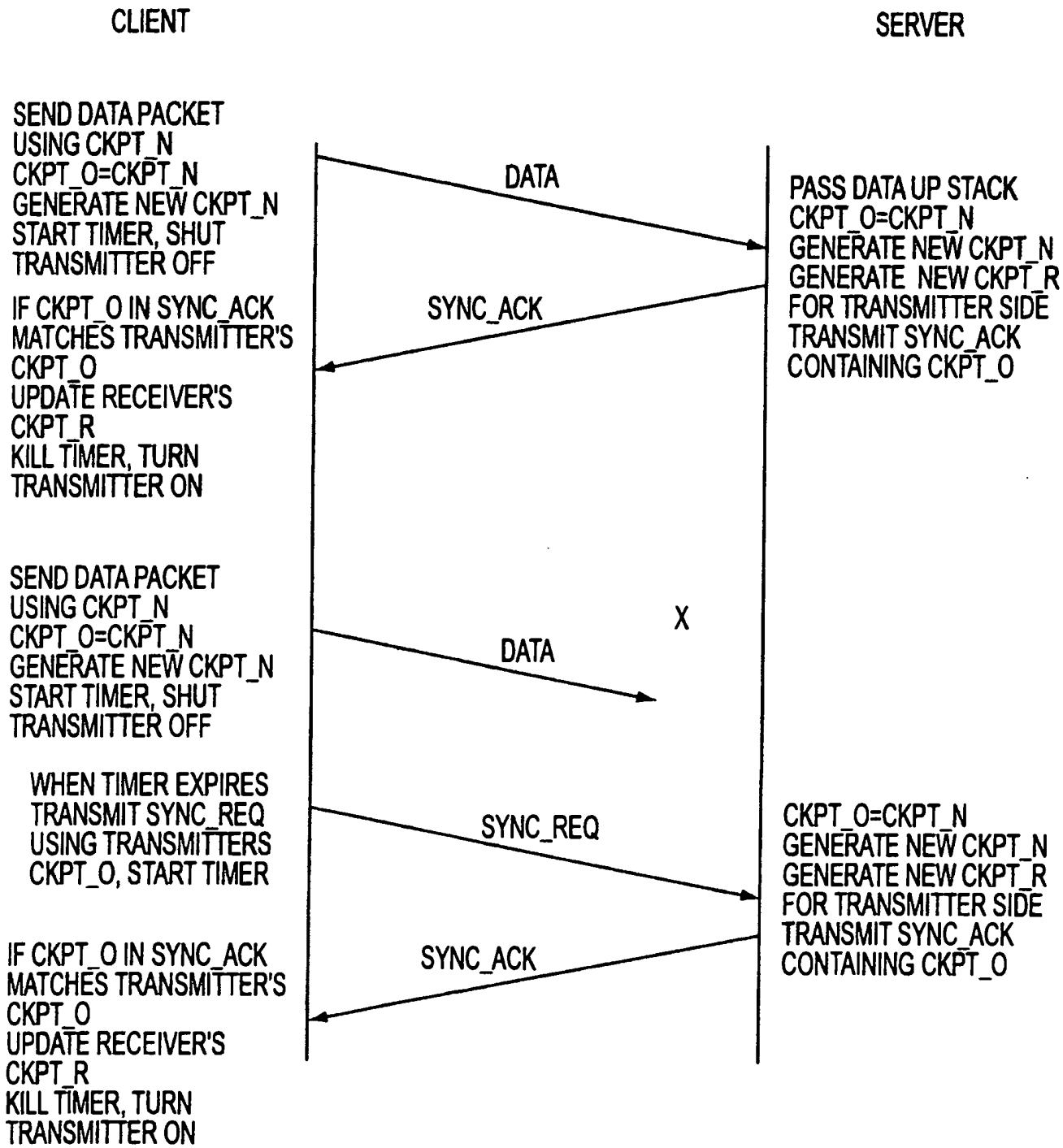

CLIENT
SERVER
SEND DATA PACKET
USING CKPT_N
CKPT_O=CKPT_N
GENERATE NEW CKPT_N
START TIMER, SHUT
TRANSMITTER OFF
DATA
PASS DATA UP STACK
CKPT_O=CKPT_N
GENERATE NEW CKPT_N
GENERATE NEW CKPT_R
FOR TRANSMITTER SIDE
TRANSMIT SYNC_ACK
CONTAINING CKPT_O
IF CKPT_O IN SYNC_ACK
MATCHES TRANSMITTER'S
CKPT_O
UPDATE RECEIVER'S
CKPT_R
KILL TIMER, TURN
TRANSMITTER ON
SYNC_ACK
SEND DATA PACKET
USING CKPT_N
CKPT_O=CKPT_N
GENERATE NEW CKPT_N
START TIMER, SHUT
TRANSMITTER OFF
X
DATA
WHEN TIMER EXPIRES
TRANSMIT SYNC_REQ
USING TRANSMITTERS
CKPT_O, START TIMER
SYNC_REQ
CKPT_O=CKPT_N
GENERATE NEW CKPT_N
GENERATE NEW CKPT_R
FOR TRANSMITTER SIDE
TRANSMIT SYNC_ACK
CONTAINING CKPT_O
IF CKPT_O IN SYNC_ACK
MATCHES TRANSMITTER'S
CKPT_O
UPDATE RECEIVER'S
CKPT_R
KILL TIMER, TURN
TRANSMITTER ON
SYNC_ACK

FIG. 32

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 August 2001 (23.08.2001)

PCT

(10) International Publication Number
WO 01/061922 A3

(51) International Patent Classification[7]: H04L 12/56, 29/06, 12/46

(21) International Application Number: PCT/US01/04340

(22) International Filing Date: 12 February 2001 (12.02.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/504,783 15 February 2000 (15.02.2000) US

(63) Related by continuation (CON) or continuation-in-part (CIP) to earlier application:
US 09/504,783 (CON)
Filed on 15 February 2000 (15.02.2000)

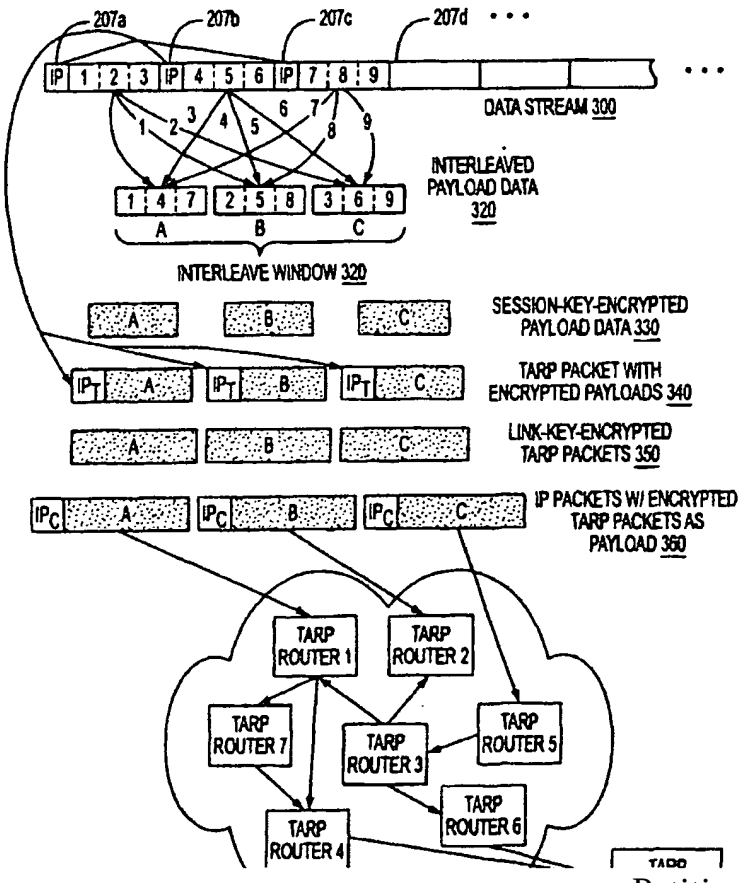
(71) Applicant *(for all designated States except US)*: **SCIENCE APPLICATIONS INTERNATIONAL CORPORATION** [US/US]; 10260 Campus Point Drive, San Diego, CA 92121 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **MUNGER, Edmund, Colby** [US/US]; 1101 Opaca Court, Crownsville, MD 21032 (US). **SCHMIDT, Douglas, Charles** [US/US]; 230 Oak Court, Severna Park, MD 21146 (US). **SHORT, Robert, Dunham, III** [US/US]; 38710 Goose Creek Lane, Leesburg, VA 20175 (US). **LARSON, Victor** [US/US]; 12026 Lisa Marie Court, Fairfax, VA 22033 (US). **WILLIAMSON, Michael** [US/US]; 26203 Ocala Circle, South Riding, VA 20152 (US).

(74) Agents: **WRIGHT, Bradley, C.** et al.; Banner & Witcoff, Ltd., 11th Floor, 1001 G Street, N.W., Washington, DC 20001-4597 (US).

[Continued on next page]

(54) Title: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY



(57) Abstract: A plurality of computer nodes communicate using seemingly random Internet Protocol source and destination addresses. Data packets matching criteria defined by a moving window of valid addresses are accepted for further processing, while those that do not meet the criteria are quickly rejected. Improvements to the basic design include (1) a load balancer that distributes packets across different transmission paths according to transmission path quality; (2) a DNS proxy server that transparently creates a virtual private network in response to a domain name inquiry; (3) a large-to-small link bandwidth management feature that prevents denial-of-service attacks at system chokepoints; (4) a traffic limiter that regulates incoming packets by limiting the rate at which a transmitter can be synchronized with a receiver; and (5) a signaling synchronizer that allows a large number of nodes to communicate with a central node by partitioning the communication function between two separate entities.

WO 01/061922 A3

(81) **Designated States** *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) **Designated States** *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

(88) **Date of publication of the international search report:**
6 March 2003

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/56 H04L29/06 H04L12/46

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, INSPEC, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 858 189 A (HITACHI LTD) 12 August 1998 (1998-08-12) column 6, line 35 -column 10, line 13 — -/--	1-27

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 August 2002	20. 08. 2002
Name and mailing address of the ISA	Authorized officer

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	MURTHY ET AL: "Congestion-oriented shortest multipath routing" PROCEEDINGS OF IEEE INFOCOM 1996. CONFERENCE ON COMPUTER COMMUNICATIONS. FIFTEENTH ANNUAL JOINT CONFERENCE OF THE IEEE COMPUTER AND COMMUNICATIONS SOCIETIES. NETWORKING THE NEXT GENERATION. SAN FRANCISCO, MAR. 24 - 28, 1996, PROCEEDINGS OF INFOCOM, L, vol. 2 CONF. 15, 24 March 1996 (1996-03-24), pages 1028-1036, XP010158171 ISBN: 0-8186-7293-5 abstract page 1028, left-hand column, line 38 -right-hand column, line 29	1-27
E	WO 01 50688 A (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)) 12 July 2001 (2001-07-12) page 11, line 18 -page 13, line 21	28,29,34
A	WO 98 59470 A (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)) 30 December 1998 (1998-12-30) page 4, line 5 -page 5, line 2	28-39
X	WO 99 48303 A (CISCO TECHNOLOGY, INC.) 23 September 1999 (1999-09-23) page 1, line 8 -page 2, line 5 page 5, line 33 -page 6, line 15 page 7, line 21 - line 33	40,50
A		41-49, 51-59
A	JONES JIM ET AL: "Distributed Denial of Service Attacks: Defenses" INTERNET ARTICLE, 'Online! 2000, XP002208785 Retrieved from the Internet: <URL:www.bai.org/pdf/DDOS-defense.pdf > 'retrieved on 2002-08-05! paragraph '0005!	60-66
X	WO 99 38081 A (ASCEND COMMUNICATIONS INC) 29 July 1999 (1999-07-29) page 9, line 13 -page 10, line 17 page 11, line 10 -page 12, line 2	67
A		68-71

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 01/04340

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-27

   A system and a method to balance the load between communication paths with varying transmission quality.

2. Claims: 28-39

   A system and a method to prevent someone from learning requested IP addresses by intercepting DNS requests.

3. Claims: 40-59

   A method to prevent a denial-of-service attack from an unauthenticated user flooding dummy data packets on to a low bandwidth link.

4. Claims: 60-66

   A method to prevent an authenticated user residing within a secure system from flooding it with dummy data packets.

5. Claims: 67-71

   A method to allocate memory in a central computer communicating with a potentially large number of client computers.

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0858189 A	12-08-1998	JP 10224400 A	21-08-1998
		EP 0858189 A2	12-08-1998
		US 6112248 A	29-08-2000
WO 0150688 A	12-07-2001	SE 517217 C2	07-05-2002
		AU 2564501 A	16-07-2001
		WO 0150688 A1	12-07-2001
		SE 9904841 A	30-06-2001
		US 2001006523 A1	05-07-2001
WO 9859470 A	30-12-1998	AU 8052398 A	04-01-1999
		SE 9702385 A	24-12-1998
		WO 9859470 A2	30-12-1998
WO 9948303 A	23-09-1999	AU 3098299 A	11-10-1999
		WO 9948303 A2	23-09-1999
WO 9938081 A	29-07-1999	US 6055575 A	25-04-2000
		AU 2562599 A	09-08-1999
		CA 2318267 A1	29-07-1999
		EP 1064602 A1	03-01-2001
		WO 9938081 A1	29-07-1999

Best Available Copy

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

OPAP IAP23 MAR 2 3 2012 PATENT & TRADEMARK OFFICE

CERTIFICATION STATEMENT

[X] Under 37 C.F.R. 1.98(d), copies of all patent, publication, pending U.S. application or other information that was previously submitted to, or cited by the USPTO in an earlier application are not required. Applicant will provide copies of the previously submitted references at the Examiner's request. **Enclosed are copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).**

This application claims priority from and is a continuation of a co-pending U.S. Application No. 13/049,552, filed March 16, 2011, which is a continuation of U.S. Application No. 11/840,560, filed August 17, 2007, now U.S. Patent No. 7,921,211, which is a continuation of U.S. Application No. 10/714,849, filed November 18, 2003, now U.S. Patent No. 7,418,504, which is a continuation of U.S. Application No. 09/558,210, filed April 26, 2000, now abandoned, which is a continuation-in-part of U.S. Application No. 09/504,783, filed on February 15, 2000, now U.S. Patent No. 6,502,135, issued December 31, 2002.

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[ ] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[X] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

Date: 3/22/12

03/27/2012 HVUONG1 00000012 501133 13336790
01 FC:1806 180.00 DA

DM_US 32511456-1.077580.0151

OPAP
MAR 2 3 2012
IAP23
PATENT & TRADEMARK OFFICE

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

OPAP
MAR 2 3 2012
IAP23
PATENT & TRADEMARK OFFICE

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc Code: TRAN.LET
Document Description: Transmittal Letter

PTO/SB/21 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

OPAP
MAR 23 2012
PATENT & TRADEMARK OFFICE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission: 52

Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Attorney Docket Number	077580-0151 (VRNK-0001CP3CNFT1)

ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
  - [x] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [x] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [x] Other Enclosure(s) (please Identify below):

Remarks

16 Boxes which include copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	McDermott, Will and Emery		
Signature			
Printed name	Toby H. Kusmer		
Date	March 23, 2012	Reg. No.	26,408

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name		Date	

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

MAR 23 2012
PATENT & TRADEMARK OFFICE

PTO/SB/17 (09-11)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

FEE TRANSMITTAL

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Examiner Name	Krisna Lim
Art Unit	2453
Attorney Docket No.	77580-151 VRNK-0001CP3CNFT1

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 180.00

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☑ Deposit Account Deposit Account Number: 50-1133 Deposit Account Name: McDermott, Will and Emery

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☑ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, except for the filing fee

☑ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☐ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
		Small Entity		Small Entity		Small Entity	
Application Type	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fees Paid ($)
Utility	380	190	620	310	250	125	
Design	250	125	120	60	160	80	
Plant	250	125	380	190	200	100	
Reissue	380	190	620	310	750	375	
Provisional	250	125	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	60	30
Each independent claim over 3 (including Reissues)	250	125
Multiple dependent claims	450	225

Total Claims _____ - 20 or HP = _____ x Fee ($) _____ = Fee Paid ($) _____

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims _____ - 3 or HP = _____ x Fee ($) _____ = Fee Paid ($) _____

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims Fee ($) _____ Fee Paid ($) _____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets _____ - 100 = _____ Extra Sheets _____ / 50 = _____ Number of each additional 50 or fraction thereof (round up to a whole number) x Fee ($) _____ = Fee Paid ($) _____

4. OTHER FEE(S)

	Fees Paid ($)
Non-English Specification, $130 fee (no small entity discount)	
Other (e.g., late filing surcharge): Information Disclosure Statement Filing Fee	$180.00

SUBMITTED BY

Signature		Registration No. (Attorney/Agent) 26,418	Telephone 617-535-4000
Name (Print/Type)	Toby H. Kusmer		Date March 23, 2012

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Applicant: Victor Larson. Docket #: 077580-0151 (VRNK-0001CP3CNFT1

Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES Serial/Reg./Patent No. 13/336,790

Date Sent: March 23, 2012 ☐ Hand Carried ☐ Fax ☐ Electronic ☐ Cert. of Mailing ☒ Express Mail Nos.

EV643771728US
EV643771731US
EV643771743US
EV643771759US
EV643771762US
EV643771776US
EV643771802US
EV643771816US
EV643771780US
EV643771793US

☒ Transmittal Letter

X IDS FORM 1449 (50 pages)

X 16 Boxes of cited references (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).

☒ Fee Transmittal

☐ Response to Missing Parts Notice

☐ Copy of Missing Parts Notice

☐ Replacement Drawing

☐ Maintenance Fee for _____years after grant

☐ Fee Address Indication Form

☐ Terminal Disclaimer

☐ Petition to Commissioner

☐ Status Inquiry

☒ Other RETURN POSTCARD

Check for $	0	☐ Charge Deposit Acct. 50-1133		Atty Init.	THK	Tkpr. #	5470	Secy. or PL:	K. Jones

CMS
Descrip.:

THE PATENT AND TRADEMARK OFFICE DATE STAMPED HEREON IS ACKNOWLEDGEMENT THAT THE ITEMS, CHECKED ABOVE, WERE RECEIVED BY THE PTO ON THE DATE STAMPED.

Accounting

3/26/12 3-26-12 1FW

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

OPAP IAP23 MAR 23 2012 PATENT & TRADEMARK OFFICE

CERTIFICATION STATEMENT

[X] Under 37 C.F.R. 1.98(d), copies of all patent, publication, pending U.S. application or other information that was previously submitted to, or cited by the USPTO in an earlier application are not required. Applicant will provide copies of the previously submitted references at the Examiner's request. **Enclosed are copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).**

This application claims priority from and is a continuation of a co-pending U.S. Application No. 13/049,552, filed March 16, 2011, which is a continuation of U.S. Application No. 11/840,560, filed August 17, 2007, now U.S. Patent No. 7,921,211, which is a continuation of U.S. Application No. 10/714,849, filed November 18, 2003, now U.S. Patent No. 7,418,504, which is a continuation of U.S. Application No. 09/558,210, filed April 26, 2000, now abandoned, which is a continuation-in-part of U.S. Application No. 09/504,783, filed on February 15, 2000, now U.S. Patent No. 6,502,135, issued December 31, 2002.

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[ ] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[X] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Date: 3/22/12

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

03/27/2012 HVUONG1 00000012 501133 13336790
01 FC:1806 180.00 DA

DM_US 32511456-1.077580.0151

OPAP
MAR 23 2012
IAP23
PATENT & TRADEMARK OFFICE

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

OPAP IAP23
MAR 23 2012
PATENT & TRADEMARK OFFICE

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc Code: TRAN.LET
Document Description: Transmittal Letter

PTO/SB/21 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

OPAS
MAR 23 2012
PATENT & TRADEMARK OFFICE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission	52

Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Attorney Docket Number	077580-0151 (VRNK-0001CP3CNFT1)

ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
  - [x] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [x] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [x] Other Enclosure(s) (please Identify below):

Remarks

16 Boxes which include copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	McDermott, Will and Emery		
Signature	/Toby H. Kusmer/		
Printed name	Toby H. Kusmer		
Date	March 23, 2012	Reg. No.	26,408

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name		Date	

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

MAR 23 2012
PATENT & TRADEMARK OFFICE

PTO/SB/17 (09-11)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

FEE TRANSMITTAL

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Examiner Name	Krisna Lim
Art Unit	2453
Attorney Docket No.	77580-151 VRNK-0001CP3CNFT1

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 180.00

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☑ Deposit Account Deposit Account Number: 50-1133 Deposit Account Name: McDermott, Will and Emery

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☑ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**

☑ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☐ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

Application Type	FILING FEES Fee ($)	FILING FEES Small Entity Fee ($)	SEARCH FEES Fee ($)	SEARCH FEES Small Entity Fee ($)	EXAMINATION FEES Fee ($)	EXAMINATION FEES Small Entity Fee ($)	Fees Paid ($)
Utility	380	190	620	310	250	125	
Design	250	125	120	60	160	80	
Plant	250	125	380	190	200	100	
Reissue	380	190	620	310	750	375	
Provisional	250	125	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	60	30
Each independent claim over 3 (including Reissues)	250	125
Multiple dependent claims	450	225

Total Claims	Extra Claims	Fee ($)	Fee Paid ($)
_____ - 20 or HP =	_____	x _____	= _____

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims	Extra Claims	Fee ($)	Fee Paid ($)
_____ - 3 or HP =	_____	x _____	= _____

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims Fee ($)	Multiple Dependent Claims Fee Paid ($)
_____	_____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof	Fee ($)	Fee Paid ($)
_____ - 100 =	_____ / 50 =	_____ (round up to a whole number)	x _____	= _____

4. OTHER FEE(S)

	Fees Paid ($)
Non-English Specification, $130 fee (no small entity discount)	
Other (e.g., late filing surcharge): Information Disclosure Statement Filing Fee	$180.00

SUBMITTED BY

Signature		Registration No. (Attorney/Agent) 26,418	Telephone 617-535-4000
Name (Print/Type)	Toby H. Kusmer		Date March 23, 2012

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Applicant: Victor Larson. Docket #. 077580-0151 (VRNK-0001CP3CNFT1

Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES Serial/Reg./Patent No. 13/336,790

Date Sent: March 23, 2012 ☐ Hand Carried ☐ Fax ☐ Electronic ☐ Cert. of Mailing ☒ Express Mail Nos.

EV643771728US
EV643771731US
EV643771743US
EV643771759US
EV643771762US
EV643771776US
EV643771802US
EV643771816US
EV643771780US
EV643771793US

☒ Transmittal Letter

X	IDS FORM 1449 (50 pages)	☐	Maintenance Fee for _____years after grant
X	16 Boxes of cited references (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).	☐	Fee Address Indication Form
☒	Fee Transmittal	☐	Terminal Disclaimer
☐	Response to Missing Parts Notice	☐	Petition to Commissioner
☐	Copy of Missing Parts Notice	☐	Status Inquiry
☐	Replacement Drawing	☒	Other RETURN POSTCARD

Check for $	0	☐ Charge Deposit Acct. 50-1133		Atty Init.	THK	Tkpr. #	5470	Secy. or PL:	K. Jones

CMS
Descrip.:

THE PATENT AND TRADEMARK OFFICE DATE STAMPED HEREON IS ACKNOWLEDGEMENT THAT THE ITEMS, CHECKED ABOVE, WERE RECEIVED BY THE PTO ON THE DATE STAMPED.

Accounting

3/26/12 3-26-12 1FV

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

OPAP IAP23 MAR 2 3 2012 PATENT & TRADEMARK OFFICE

CERTIFICATION STATEMENT

[X] Under 37 C.F.R. 1.98(d), copies of all patent, publication, pending U.S. application or other information that was previously submitted to, or cited by the USPTO in an earlier application are not required. Applicant will provide copies of the previously submitted references at the Examiner's request. **Enclosed are copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).**

This application claims priority from and is a continuation of a co-pending U.S. Application No. 13/049,552, filed March 16, 2011, which is a continuation of U.S. Application No. 11/840,560, filed August 17, 2007, now U.S. Patent No. 7,921,211, which is a continuation of U.S. Application No. 10/714,849, filed November 18, 2003, now U.S. Patent No. 7,418,504, which is a continuation of U.S. Application No. 09/558,210, filed April 26, 2000, now abandoned, which is a continuation-in-part of U.S. Application No. 09/504,783, filed on February 15, 2000, now U.S. Patent No. 6,502,135, issued December 31, 2002.

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[ ] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[X] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Date: 3/22/12

03/27/2012 HVUONG1 00000012 501133 13336790

01 FC:1806 180.00 DA

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

DM_US 32511456-1.077580.0151

OPAP
MAR 2 3 2012
IAP23
PATENT & TRADEMARK OFFICE

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

OPAP IAP23
MAR 23 2012
PATENT & TRADEMARK OFFICE

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc Code: TRAN.LET
Document Description: Transmittal Letter

PTO/SB/21 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

OPAP
MAR 23 2012
PATENT & TRADEMARK OFFICE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission	52

Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Attorney Docket Number	077580-0151 (VRNK-0001CP3CNFT1)

ENCLOSURES *(Check all that apply)*

- [✓] Fee Transmittal Form
  - [✓] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [✓] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [✓] Other Enclosure(s) (please Identify below):

Remarks

16 Boxes which include copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	McDermott, Will and Emery		
Signature	/Toby H. Kusmer/		
Printed name	Toby H. Kusmer		
Date	March 23, 2012	Reg. No.	26,408

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name		Date	

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

MAR 23 2012 IAP23
PATENT & TRADEMARK OFFICE

PTO/SB/17 (09-11)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

FEE TRANSMITTAL

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Examiner Name	Krisna Lim
Art Unit	2453
Attorney Docket No.	77580-151 VRNK-0001CP3CNFT1

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 180.00

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☑ Deposit Account Deposit Account Number: 50-1133 Deposit Account Name: McDermott, Will and Emery

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☑ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**

☑ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☐ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

Application Type	FILING FEES Fee ($)	FILING FEES Small Entity Fee ($)	SEARCH FEES Fee ($)	SEARCH FEES Small Entity Fee ($)	EXAMINATION FEES Fee ($)	EXAMINATION FEES Small Entity Fee ($)	Fees Paid ($)
Utility	380	190	620	310	250	125	
Design	250	125	120	60	160	80	
Plant	250	125	380	190	200	100	
Reissue	380	190	620	310	750	375	
Provisional	250	125	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	60	30
Each independent claim over 3 (including Reissues)	250	125
Multiple dependent claims	450	225

Total Claims _____ - 20 or HP = _____ x Fee ($) _____ = Fee Paid ($) _____

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims _____ - 3 or HP = _____ x Fee ($) _____ = Fee Paid ($) _____

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims Fee ($) _____ Fee Paid ($) _____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets _____ - 100 = Extra Sheets _____ / 50 = Number of each additional 50 or fraction thereof _____ (round up to a whole number) x Fee ($) _____ = Fee Paid ($) _____

4. OTHER FEE(S)

Fees Paid ($)

Non-English Specification, $130 fee (no small entity discount) _____

Other (e.g., late filing surcharge): Information Disclosure Statement Filing Fee $180.00

SUBMITTED BY

Signature		Registration No. (Attorney/Agent) 26,418	Telephone 617-535-4000
Name (Print/Type)	Toby H. Kusmer		Date March 23, 2012

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Applicant: Victor Larson. Docket #. 077580-0151 (VRNK-0001CP3CNFT1

Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES Serial/Reg./Patent No. 13/336,790

Date Sent: March 23, 2012 ☐ Hand Carried ☐ Fax ☐ Electronic ☐ Cert. of Mailing ☒ Express Mail Nos.

EV643771728US
EV643771731US
EV643771743US
EV643771759US
EV643771762US
EV643771776US
EV643771802US
EV643771816US
EV643771780US
EV643771793US

☒ Transmittal Letter

X	IDS FORM 1449 (50 pages)	☐	Maintenance Fee for _____years after grant
X	16 Boxes of cited references (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).	☐	Fee Address Indication Form
☒	Fee Transmittal	☐	Terminal Disclaimer
☐	Response to Missing Parts Notice	☐	Petition to Commissioner
☐	Copy of Missing Parts Notice	☐	Status Inquiry
☐	Replacement Drawing	☒	Other RETURN POSTCARD

Check for $	0	☐ Charge Deposit Acct. 50-1133		Atty Init.	THK	Tkpr. #	5470	Secy. or PL:	K. Jones

CMS
Descrip.:

THE PATENT AND TRADEMARK OFFICE DATE STAMPED HEREON IS ACKNOWLEDGEMENT THAT THE ITEMS, CHECKED ABOVE, WERE RECEIVED BY THE PTO ON THE DATE STAMPED.

Accounting

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	**13/336,790**
Filing Date	**12-23-2011**
First Named Inventor	**Victor Larson**
Art Unit	**2165**
Examiner Name	**Krisna Lim**
Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A161	6,131,121	10/10/2000	Mattaway et al.	
	A162	6,499,108	12/24/2002	Johnson	

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes-Number-Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	A1112	ITU-T Recommendation H.323, "Infrastructure of Audiovisual Services – Systems and Terminal Equipment for Audiovisual Services. Packet-Based Multimedia Communications System," International Telecommunications Union, pages 1-128, February 1998	
	A1113	ITU-T Recommendation H.225.0, "Infrastructure of Audiovisual Services – Transmission Multiplexing and Synchronization. Call Signaling Protocols and Media Stream Packetization for Packet-Based Multimedia Communication systems," International Telecommunication Union, pages 1-155, February 1998	
	A1114	ITU-T Recommendation H.235, "Infrastructure of Audiovisual Services – Systems Aspects. Security and Encryption for H-Series (H.323 and other H.245-based) Multimedia Terminals," International Telecommunication Union, pages 1-39, February 1998	
	A1115	ITU-T Recommendation H.245, "Infrastructure of Audiovisual Services – Communication Procedures. Control Protocol for Multimedia Communication," International Telecommunication Union, pages 1-280, February 1998	
	A1116	Request for Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No.8,051,181)	
	A1117	Transmittal Letters (Patent No.8,051,181)	
	A1118	Exhibit X5, Droms, R., RFC 2131, "Dynamic Host Configuration Protocol," 1987	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[X] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[ ] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Date: 4/24/12

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

DM_US 33806475-1.077580.0151

Electronic Acknowledgement Receipt

EFS ID:	12623744
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kerrie Jones
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	25-APR-2012
Filing Date:	23-DEC-2011
Time Stamp:	11:16:47
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	75951 da7d1f9616c8a3e06b11caf201867c796526008c	no	2

Warnings:	
Information:	

This is not an USPTO supplied IDS fillable form					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
2	Non Patent Literature	D1112.pdf	6631563 906ff6daf56bfcc31393b154a52c600e04b0a378	no	129
Warnings:					
Information:					
3	Non Patent Literature	D1113.pdf	8752435 96293b2d311e620715c85cde849c7068873078e7	no	156
Warnings:					
Information:					
4	Non Patent Literature	D1114.pdf	2184536 2d5897e60d1e96ef708bd7248d1a4f52dab66814	no	40
Warnings:					
Information:					
5	Non Patent Literature	D1115.pdf	13279514 06c632218653419b404c6dd372a83acad284c62b	no	281
Warnings:					
Information:					
6	Non Patent Literature	D1116.pdf	18717491 82d8e4078df503f9f1b03f6fa1ab864a0d2ab00a	no	320
Warnings:					
Information:					
7	Non Patent Literature	D1117.pdf	90402 47ee405fbb7f1e62fd6e4793a276d820608be91d	no	3
Warnings:					
Information:					
8	Non Patent Literature	D1118.pdf	2054150 923ded65634628a0c2bb97275d15e8939e6101f1	no	40
Warnings:					
Information:					
		Total Files Size (in bytes):	51786042		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	**13/336,790**
Filing Date	**12-23-2011**
First Named Inventor	**Victor Larson**
Art Unit	**2165**
Examiner Name	**Krisna Lim**
Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes3–Number 4–Kind Codes5 (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	A1119	Hopen Transcript dated April 11, 2012	
	A1120	VirnetX Claim Construction Opinion	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[X] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[ ] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Toby H. Kusmer, Reg. No. 40,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

Date: May 3, 2012

DM_US 34023885-1.077580.0151

Electronic Acknowledgement Receipt

EFS ID:	12699070
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kerrie Jones
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	03-MAY-2012
Filing Date:	23-DEC-2011
Time Stamp:	16:56:09
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	63176 1f57b95d5998a29578b306dd80140fe3675 20834	no	2

Warnings:	
Information:	

This is not an USPTO supplied IDS fillable form					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
2	Non Patent Literature	D1119.pdf	2878466 8b71e4b3742f29ed35c56c766502d527a0ddf2bb	no	57
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
3	Non Patent Literature	D1120.pdf	533111 a82b1ad1fb1fb3bddbe19efd0f1f957db8e54c55	no	31
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
Total Files Size (in bytes):			3474753		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	**13/336,790**
Filing Date	**12-23-2011**
First Named Inventor	**Victor Larson**
Art Unit	**2165**
Examiner Name	**Krisna Lim**
Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes-Number-Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	A1121	Declaration of Angelos D. Keromytis, Ph.D.	
	A1122	Declaration of Dr. Robert Dunham Short III	
	A1123	Exhibit A-1, Verdict Form from VirnetX, Inc. v. Microsoft Corp., No. 6:07-CV-80 (E.D. Tex.)	
	A1124	Exhibit A-3, Declaration of Jason Nieh, Ph.D. (Control No. 95/001,269)	
	A1125	Exhibit A-4, Redacted Deposition of Chris Hopen from VirnetX, Inc. v. Cisco Systems, Inc., No. 6:07-CV 417 (E.D. Tex. April 11, 2012)	
	A1126	Exhibit B-1, Excerpt from Deposition of Defense FY 2000/2001 Biennial Budget Estimates, (Feb. 1999)	
	A1127	Exhibit B-2, Collection of Reports and Presentations on DARPA Projects	
	A1128	Exhibit B-3, Maryann Lawlor, Transient Partnerships Stretch Security Policy Management, Signal Magazine (Sept. 2001) http://www.afcea.org/signal/articles/anmviewer.asp?a=494&print=yes	
	A1129	Joel Snyder, Living in Your Own Private Idaho, Network World (January 28, 1998) http://www.networkworld.com/intranet/0126review.html.	
	A1130	Time Greene, CEO's Chew the VPN Fat, CNN.com (June 17, 1999), http://www.cnn.com/TECH/computing/9906/17/vpnfat.ent.idg/index.html?iref=allsearch	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[X] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[ ] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Date: 5/18/12

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

DM_US 35089818-1.077580.0151

Electronic Acknowledgement Receipt

EFS ID:	12822659
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kerrie Jones
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	21-MAY-2012
Filing Date:	23-DEC-2011
Time Stamp:	13:09:25
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	73771 1071c63a96babb5dc59498dfa463fc246252d8d6	no	2

Warnings:	
Information:	

This is not an USPTO supplied IDS fillable form

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

2	Non Patent Literature	D1121.pdf	4301486 cb320cd4e2284187bad62b1dcc5985f9a30fc2ae	no	98

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

3	Non Patent Literature	D1122.pdf	235218 1ee5e74886cc86d9669ccefb0e913ab95d7ab123	no	6

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

4	Non Patent Literature	D1123.pdf	78623 8e809ede185d2847d6fe215a8f1b281e9df11a70	no	3

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

5	Non Patent Literature	D1124.pdf	424402 929e7bf435c6276ef913af84eb6aa5e9f5014ebc	no	9

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

6	Non Patent Literature	D1125.pdf	186247 4bf903af938028fc72f6cabbcc8efb2f788bc6b6	no	5

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

7	Non Patent Literature	D1126.pdf	987245 2f6bdc05cf88407b211635be0a65eaaaad52878c	no	23

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

8	Non Patent Literature	D1127.pdf	5974350 66f2a38a997c8dc339f848fb04a4ef68df80bfb4	no	95
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
9	Non Patent Literature	D1128.pdf	351127 3f824e2ea0a2cf055600561add2b717e1ed56cd9	no	5
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
10	Non Patent Literature	D1129.pdf	298881 e6ef10c93c51f5e3ca0af7ea9d2bd99cea9550fd	no	5
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
11	Non Patent Literature	D1130.pdf	273615 9ba7c10abcf45b09e617216e4bf1aa755b31931c	no	6
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
		Total Files Size (in bytes):	13184965		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronic Acknowledgement Receipt

EFS ID:	12912054
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kerrie Jones
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	01-JUN-2012
Filing Date:	23-DEC-2011
Time Stamp:	12:39:55
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	D1190.pdf	1334655 db4f0de7fd0cbf541b8b1f07a5be78f2d57735f7	no	35

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
2	Non Patent Literature	D1191.pdf	1685850 d202562b825d6fb1fad06ab48ccc32894a96fad4	no	64
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
3	Non Patent Literature	D1193.pdf	1092988 f3c54e9f23c88cb4e7ea577d4eadf08df78f62e1	no	41
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
4	Non Patent Literature	D1194.pdf	475905 b6252dcf3fc6dccd1385f322612c124f06ae60d3	no	19
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
5	Non Patent Literature	D1195.pdf	902251 63bd1d7c6cdd131cd34a3ef3cd6baa2a6b9427c1	no	33
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
6	Non Patent Literature	D1196.pdf	462285 bb47612f473098de515196ff5df486a469e85166	no	17
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
7	Non Patent Literature	D1197.pdf	1290635 88c9dd3dfa5d66a114f5ba617af038121c2f468b	no	48
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					

8	Non Patent Literature	D1198.pdf	1300599 f58d460ea5bdd7f390859ccc146a6e7e3f78fd1f	no	48
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
9	Non Patent Literature	D1199.pdf	637158 162acfa69253dd96c63c9b2a7e33333ec3031ab6	no	24
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
10	Non Patent Literature	D1200.pdf	697066 4c3e7fa216a865ddfe596077941d8f1c80bfafb4	no	24
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
11	Non Patent Literature	D1192.pdf	538172 ae3fb0669fe7d52f5efae5364185a7f31e440e7a	no	39
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
		Total Files Size (in bytes):	10417564		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes–Number–Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER 'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D1131	Peter Alexander Invalidity Report	
	D1132	Defendants' Second Supplemental Joint Invalidity Contentions	
	D1133	Exhibit 118A, Altiga VPN System[1] vs. Claims of the '135 Patent [2]	
	D1134	Exhibit 119A, Altiga VPN System[1] vs. Claims of the '151 Patent [2]	
	D1135	Exhibit 120A, Altiga VPN System[1] vs. Claims of the '180 Patent [2]	
	D1136	Exhibit 121A, Altiga VPN System[1] vs. Claims of the '211 Patent [2]	
	D1137	Exhibit 122A, Altiga VPN System[1] vs. Claims of the '504 Patent [2]	
	D1138	Exhibit 123A, Altiga VPN System[1] vs. Claims of the '759 Patent [2]	
	D1139	Exhibit 12A, SSL 3.0[1] vs. Claims of the '135 Patent[2]	
	D1140	Exhibit 13A, SSL 3.0[1] vs. Claims of the '504 Patent[2]	
	D1141	Exhibit 14A, SSL 3.0[1] vs. Claims of the '211 Patent[2]	
	D1142	Exhibit 228A, Understanding OSF DCE 1.1 for AIX and OS/2[1] (APP_VX0556531-804) vs. Claims of the '135 Patent[2]	
	D1143	Exhibit 229A, Understanding OSF DCE 1.1 for AIX and OS/2[1] (APP_VX0556531-804) vs. Claims of the '151 Patent[2]	
	D1144	Exhibit 230A, Understanding OSF DCE 1.1 for AIX and OS/2[1] (APP_VX0556531-804) vs. Claims of the '180 Patent[2]	
	D1145	Exhibit 231A, Understanding OSF DCE 1.1 for AIX and OS/2[1] (APP_VX0556531-804) vs. Claims of the '211 Patent[2]	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D1146	Exhibit 232A, Understanding OSF DCE 1.1 for AIX and OS/2[1] (APP_VX0556531-804) vs. Claims of the '504 Patent[2]	
	D1147	Exhibit 233A, Understanding OSF DCE 1.1 for AIX and OS/2[1] (APP_VX0556531-804) vs. Claims of the '759 Patent[2]	
	D1148	Exhibit 255, Schulzrinne[1] vs. Claims of the '135 Patent[2]	
	D1149	Exhibit 256, Schulzrinne[1] vs. Claims of the '504 Patent[2]	
	D1150	Exhibit 257, Schulzrinne[1] vs. Claims of the '211 Patent[2]	
	D1151	Exhibit 258, Schulzrinne[1] vs. Claims of the '151 Patent[2]	
	D1152	Exhibit 259, Schulzrinne[1] vs. Claims of the '180 Patent[2]	
	D1153	Exhibit 260, Schulzrinne[1] vs. Claims of the '759 Patent[2]	
	D1154	Exhibit 261, SSL 3.0[1] vs. Claims of the '151 Patent[2]	
	D1155	Exhibit 262, SSL 3.0[1] vs. Claims of the '759 Patent[2]	
	D1156	Exhibit 263, Wang[1] vs. Claims of the '135 Patent[2]	
	D1157	Wang[1] vs. Claims of the '504 Patent[2]	
	D1158	Wang[1] vs. Claims of the '211 Patent[2]	
	D1159	Exhibit 1, Alexander CV.pdf	
	D1160	Exhibit 2, Materials Considered by Peter Alexander	
	D1161	Exhibit 3, Cross Reference Chart	
	D1162	Exhibit 4, RFC 2543[1] vs. Claims of the '135 Patent	
	D1163	Exhibit 5, RFC 2543[1] vs. Claims of the '504 Patent	
	D1164	Exhibit 6, RFC 2543[1] vs. Claims of the '211 Patent	
	D1165	Exhibit 7, The Schulzrinne Presentation[1] vs. Claims of the '135 Patent	
	D1166	Exhibit 8, The Schulzrinne Presentation[1] vs. Claims of the '504 Patent	
	D1167	Exhibit 9, The Schulzrinne Presentation[1] vs. Claims of the '211 Patent	
	D1168	Exhibit 10, The Schulzrinne Presentation[1] vs. Claims of the '151 Patent	
	D1169	Exhibit 11, The Schulzrinne Presentation[1] vs. Claims of the '180 Patent	
	D1170	Exhibit 12, The Schulzrinne Presentation[1] vs. Claims of the '759 Patent	
	D1171	Exhibit 13, SSL 3.0[2] vs. Claims of the '135 Patent	
	D1172	Exhibit 14, SSL 3.0[2] vs. Claims of the '504 Patent	
	D1173	Exhibit 15, SSL 3.0[2] vs. Claims of the '211 Patent	
	D1174	Exhibit 16, SSL 3.0[2] vs. Claims of the '151 Patent	
	D1175	Exhibit 17, SSL 3.0[2] vs. Claims of the '759 Patent	
	D1176	Exhibit 18, Kiuchi[1] vs. Claims of the '135 Patent	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D1177	Exhibit 19, Kiuchi[1] vs. Claims of the '504 Patent	
	D1178	Exhibit 20, Kiuchi[1] vs. Claims of the '211 Patent	
	D1179	Exhibit 21, Kiuchi[1] vs. Claims of the '151 Patent	
	D1180	Exhibit 22, Kiuchi[1] vs. Claims of the '180 Patent	
	D1181	Exhibit 23, Kiuchi[1] vs. Claims of the '759 Patent	
	D1182	Exhibit 24, U.S. Patent No. 6,119,234 (hereinafter "Aziz") and RFC 2401[2] vs. Claims of the '135 Patent	
	D1183	Exhibit 25, U.S. Patent No. 6,119,234 (hereinafter "Aziz") and RFC 2401[2] vs. Claims of the '504 Patent	
	D1184	Exhibit 26, U.S. Patent No. 6,119,234 (hereinafter "Aziz") and RFC 2401[2] vs. Claims of the '211 Patent	
	D1185	Exhibit 27, U.S. Patent No. 6,119,234 (hereinafter "Aziz") and RFC 2401[2] vs. Claims of the '151 Patent	
	D1186	Exhibit 28	
	D1187	Exhibit 29, The Altiga System[1] vs. Claims of the '135 Patent	
	D1188	Exhibit 30, The Altiga System[1] vs. Claims of the '504 Patent	
	D1189	Exhibit 31, The Altiga System[1] vs. Claims of the '211 Patent	
	D1190	Exhibit 32, The Altiga System[1] vs. Claims of the '759 Patent	
	D1191	Exhibit 33, U.S. Patent No. 6,496,867 ("Beser")[1]and RFC 2401[2] vs. Claims of the '135 Patent	
	D1192	Exhibit 34, U.S. Patent No. 6,496,867 ("Beser")[1]and RFC 2401[2] vs. Claims of the '504 Patent	
	D1193	Exhibit 35, U.S. Patent No. 6,496,867 ("Beser")[1]and RFC 2401[2] vs. Claims of the '211 Patent	
	D1194	Exhibit 36, U.S. Patent No. 6,496,867 ("Beser")[1]and RFC 2401[2] vs. Claims of the '151 Patent	
	D1195	Exhibit 37, U.S. Patent No. 6,496,867 ("Beser")[1]and RFC 2401[2] vs. Claims of the '180 Patent	
	D1196	Exhibit 38, Kent[1] vs. Claims of the '759 Patent	
	D1197	Exhibit 39, RFC 2538, Storing Certificates in the Domain Name System (DNS)[1] vs. Claims of the '504 Patent[2]	
	D1198	Exhibit 40, RFC 2538, Storing Certificates in the Domain Name System (DNS)[1] vs. Claims of the '211 Patent[2]	
	D1199	Exhibit 41, Aziz ('646)[1] vs. Claims of the '759 Patent	
	D1200	Exhibit 42, The PIX Firewall[1] vs. Claims of the '759 Patent	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[X] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

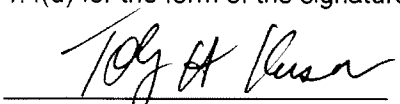
[ ] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.



Date: 6/1/12

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

DM_US 35497951-1.077580.0151

Electronic Acknowledgement Receipt

EFS ID:	12911962
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kerrie Jones
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	01-JUN-2012
Filing Date:	23-DEC-2011
Time Stamp:	12:35:14
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	130560 ba1ac2e55b673813d2ac7b8cce7cbad5c12d203b	no	4

Warnings:	
Information:	

This is not an USPTO supplied IDS fillable form

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

2	Non Patent Literature	D1131.pdf	3260103 74ef5d4512add8f0bf148558f4eb310f5e56d39f	no	220

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

3	Non Patent Literature	D1132.pdf	30634 c8723f1c4a74665a8a7b9693283fcb0105383dd6	no	3

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

4	Non Patent Literature	D1133.pdf	10059093 09aa21c9dc0c849cf1a53c96b67ec06c66510bb7	no	251

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

5	Non Patent Literature	D1134.pdf	3029226 cf4dc78e2cdc44a5ec325a160d2914dadf1dcc1f	no	73

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

6	Non Patent Literature	D1135.pdf	3134578 9de62a94d4bd8509aec73914fb5968389d04eddc	no	78

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

7	Non Patent Literature	D1136.pdf	3942265 c1aedbf7503ee346d7523817c89f9775da10e2e7	no	95

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

8	Non Patent Literature	D1137.pdf	3959945 af1fbe1d0ab2b9fda0f7525cfddd756f1441f34e	no	95
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
9	Non Patent Literature	D1138.pdf	4082758 d6503cc36bc9164429b08cff316e228f0d062f64	no	107
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
10	Non Patent Literature	D1139.Pdf	711320 5b56b9f7528e3260f32dbfa7338765723b3e9718	no	25
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
11	Non Patent Literature	D1140.pdf	941221 920e0cc8cb24927577e5affea22e15f5ea041065	no	33
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
12	Non Patent Literature	D1141.pdf	943986 cc9ce3cfea66f487906f3623efdc75f0f3ba22d5	no	33
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
13	Non Patent Literature	D1142.pdf	594440 943e8097cbccde5b79c830067081585000604cc28	no	21
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
14	Non Patent Literature	D1143.pdf	427888 dbf1cfb287d362939680b0859fdcf8a4c1c249a3	no	15
Warnings:					

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
15	Non Patent Literature	D1144.pdf	776663 17bd93d8f5d51386a2fb7f1d715d828c8c860684	no	25
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
16	Non Patent Literature	D1145.pdf	1405903 c0080dfc7643c5a1fef4738d53b563f890ee6005	no	45
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
17	Non Patent Literature	D1146.pdf	1407006 8475b7bfeb2c1744a65caf9745502e4bb2b9443f	no	44
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
18	Non Patent Literature	D1147.pdf	805076 febfef6db73530b40ff463b968fda277231c655e	no	28
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
19	Non Patent Literature	D1148.pdf	2203321 e0da9a90856cfa27f90663d6dcba447401fcc1a0	no	90
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
20	Non Patent Literature	D1149.pdf	3147948 313483b73df5bad9b7e5c585809f9e186eaf9bd4	no	122
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					

21	Non Patent Literature	D1150.pdf	3141643 004566a6bb562124250ce55d8a5c3c45d22ef9ba	no	122
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
22	Non Patent Literature	D1151.pdf	1165021 a149ceed376546bef14a2492da53c5f8659e4306	no	49
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
23	Non Patent Literature	D1152.pdf	1063902 602c401071cc6435a6e374d0425baea7ec7e2f0c	no	41
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
24	Non Patent Literature	D1153.pdf	1955096 de7e2dcc9c5d454cf44184a5e59fec0d4c19ffd6	no	74
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
25	Non Patent Literature	D1154.pdf	368908 38a2f0002d1d09600bffe5093c5b72ded5012b87	no	14
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
26	Non Patent Literature	D1155.pdf	676883 582d52501bb5fb36479accfc93474e2736526f44	no	24
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
27	Non Patent Literature	D1156.pdf	885422 50b9bc7c5f3ca481df882116c2baab4e9e0ffacb	no	59
Warnings:					

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
28	Non Patent Literature	D1157.pdf	767953 d41d24160ebdf77fdf170ab402f3435eff6ec04a	no	55
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
29	Non Patent Literature	D1158.pdf	778344 6e09d94cda3901ddad57c8134420384b8a3a62c9	no	56
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
30	Non Patent Literature	D1159.pdf	313591 a5c182ec921bf594fb6006678478eaebe2040f79	no	22
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
31	Non Patent Literature	D1160.pdf	99073 6032e737141f46ebd3af06f94412abcb83d837b8	no	16
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
32	Non Patent Literature	D1161.pdf	290550 a95d6561c60f6b9e5533045b82f99451fa21b8f6	no	24
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
33	Non Patent Literature	D1162.pdf	1071164 cefb83da7af40e4e4e1bd46131ca7c0257fd50eb	no	43
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					

34	Non Patent Literature	D1163.pdf	1235283 4a8264cf35a86a750143e5784708d2e8b2bb9eed	no	46
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
35	Non Patent Literature	D1164.pdf	1237581 c9a70fa026e3620d395a48ea295b575e0dddde442	no	46
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
36	Non Patent Literature	D1165.pdf	769860 c0d81fef0a644005773f699c729b137caad1154f	no	32
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
37	Non Patent Literature	D1166.pdf	967504 9167ee2107e7842f5dbf109778dd645e73c687d6	no	36
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
38	Non Patent Literature	D1167.pdf	800290 b3e1ebe23d038b9533000ac6dae9f22e9a48e55a	no	36
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
39	Non Patent Literature	D1168.pdf	358283 07c75d941d270787c758fb814b3275ad44a37081	no	15
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
40	Non Patent Literature	D1169.pdf	275344 86699e2f3e45e7101fc8b327707ad19a4b31330d	no	11
Warnings:					

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

41	Non Patent Literature	D1170.pdf	790998 be8a5ef43289b528b187880d172aa778c996d78f	no	29

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

42	Non Patent Literature	D1171.pdf	897777 bf7e82ab12db50ef85f6f9f78f5166184710ac08	no	33

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

43	Non Patent Literature	D1172.pdf	1029160 255f1de201cdad723b864cb2d579f346d99be789	no	38

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

44	Non Patent Literature	D1173.pdf	1027665 eea3f1926ba18599dcbd284b742b6234b0cd0e66	no	39

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

45	Non Patent Literature	D1174.pdf	233030 282372f14f4b702ec797403952907d7d987644b9	no	10

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

46	Non Patent Literature	D1175.pdf	655028 534519289371 54d4e82356be3e8bdab6c9867c03	no	25

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

47	Non Patent Literature	D1176.pdf	806842 398a53dd0e727476bd95f85158b35c9835b8fb2f	no	30
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
48	Non Patent Literature	D1177.pdf	958598 0ea4898e8747bbb25aa702f4ea36cc41ac8f0ac8	no	35
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
49	Non Patent Literature	D1178.pdf	952945 3e99f9a9a75f11b5fe496455dbb597c35eec1f3b	no	35
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
50	Non Patent Literature	D1179.pdf	194158 01b2ca2ea4cefbc9749ca83bf321aafae7382b61	no	8
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
51	Non Patent Literature	D1180.pdf	556180 be16cd1d96beead6880933a31e3c542c215307d5	no	19
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
52	Non Patent Literature	D1181.pdf	675954 0ca6204c94a3811434cb097c1501d92b0cceed8e	no	25
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
53	Non Patent Literature	D1182.pdf	1355829 5f6063f58323ad4d61b621d4a3d3368674501d54	no	51
Warnings:					

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

54	Non Patent Literature	D1183.pdf	1215891 94dbf32038c4abde2eeaced2052f624eed3cbfcb	no	45

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

55	Non Patent Literature	D1184.pdf	1202606 8fadeccb40217f01d137fe78ee9de9c5f962fea1	no	45

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

56	Non Patent Literature	D1185.pdf	448290 867cb2b1db8748dee8f96e8856c993fc08b1296e	no	18

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

57	Non Patent Literature	D1186.pdf	9426 d92dac638b115c40d00234dd5deff30818d8b016	no	2

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

58	Non Patent Literature	D1187.pdf	1452336 2b4a8e50ae71daa4c9f875ecb349217aaa287bf6	no	35

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

59	Non Patent Literature	D1188.pdf	1585677 26d9e803edc97291c064561782a680fb039ebde8	no	40

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

60	Non Patent Literature	D1189.pdf	1608409 533bc627d8237002ebc34e68da820c64f38cd4d9	no	41

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

Total Files Size (in bytes):	80872428

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes-Number-Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D1201	Exhibit A-1, Kiuchi[1] vs. Claims of the '135 Patent[2]	
	D1202	Exhibit B-1, Kiuchi[1] vs. Claims of the '211 Patent[2]	
	D1203	Exhibit C-1, Kiuchi[1] vs. Claims of the '504 Patent[2]	
	D1204	Exhibit D, Materials Considered	
	D1205	Exhibit E, Expert Report of Stuart G. Stubblebine, Ph.D.	
	D1206	Exhibit F, Expert Report of Stuart G. Stubblebine, Ph.D.	
	D1207	Exhibit G, Opening Expert Report of Dr. Stuart Stubblebine Regarding Invalidity of the '135, '211, and '504 Patents	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[X] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[ ] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

/ Toby H. Kusmer /

Date: 6/1/12

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

DM_US 35546776-1.077580.0151

Electronic Acknowledgement Receipt

EFS ID:	12915320
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kerrie Jones
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	01-JUN-2012
Filing Date:	23-DEC-2011
Time Stamp:	15:20:25
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	61663 0ee9a9f0dd2de3b804f88e80792c25f841a47b80	no	2

Warnings:	
Information:	

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
This is not an USPTO supplied IDS fillable form					
2	Non Patent Literature	D1201A.pdf	1011692 670146792fba847f89b09bd1cf5c3c8b6a41816d	no	100
Warnings:					
Information:					
3	Non Patent Literature	D1201B.pdf	1163786 72e6a8c69399fcf4c741adcf631419181971 7813	no	81
Warnings:					
Information:					
4	Non Patent Literature	D1202A.pdf	1033550 03d67d549a65b6f8d17ffd4f664f629c0902 039a	no	100
Warnings:					
Information:					
5	Non Patent Literature	D1202B.pdf	1338301 2f977e2e9c75fa95079854b9be3a7cdc9cb0 99ac	no	100
Warnings:					
Information:					
6	Non Patent Literature	D1202C.pdf	827794 d1dbd6f0e330ace1bd3b2eb104d9113ff50 a56c5	no	41
Warnings:					
Information:					
7	Non Patent Literature	D1203A.pdf	1036611 9d43da78dcf81aea6d47df735e9bef815553 7af4	no	100
Warnings:					
Information:					
8	Non Patent Literature	D1203B.pdf	1289345 5a961e0418bfd42c7a87dd7016fd8210dce cea6d	no	100
Warnings:					
Information:					
9	Non Patent Literature	D1203C.pdf	1118664 5429b9f31ebaec5271a9d2e8b6e22a6167e cf85f	no	78
Warnings:					
Information:					

10	Non Patent Literature	D1204.pdf	103729 cb05f5e2bc8b94824cd584c0216e234020d62d51	no	3
Warnings:					
Information:					
11	Non Patent Literature	D1205.pdf	134207 401222abc8109e44e80b981c192c3bb60dd0d6c9	no	19
Warnings:					
Information:					
12	Non Patent Literature	D1206.pdf	106899 225eff9edc51590a7c923fb400e5b70a1d03c27d	no	7
Warnings:					
Information:					
13	Non Patent Literature	D1207.pdf	584668 ebfbb21df2ac355190d88201f32765c5a19ff64d	no	60
Warnings:					
Information:					
		Total Files Size (in bytes):	9810909		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Victor Larson *et al.*	:	
Serial No.: 13/336,790	:	Confirmation No. 6217
Filed: December 23, 2011	:	Group Art Unit: 2453
Customer Number: 23630	:	Examiner: Lim, Krisna

For: System and Method Employing an Agile Network Protocol for Secure Communications Using Secure Domain Names

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY "A"

Sir:

This Reply is being filed in response to the Office Action mailed from the United States Patent and Trademark office on March 2, 2012.

Applicants appreciate Examiner's thorough examination of the subject application and request reconsideration and further examination in view of the following:

Claims begin on page 2 of this paper.

Remarks begin on page 6 of this paper.

Claims

The claims are being presented solely for the convenience of the Office. No claims are being added, amended, deleted, or canceled.

Claims Listing

1. (Original) A network device, comprising:

a storage device storing an application program for a secure communications service; and

at least one processor configured to execute the application program for the secure communications service so as to enable the network device to:

send a request to look up a network address of a second network device based on an identifier associated with the second network device;

receive an indication that the second network device is available for the secure communications service, the indication including the requested network address of the second network device and provisioning information for a virtual private network communication link;

connect to the second network device, using the received network address of the second network device and the provisioning information for the virtual private network communication link; and

communicate with the second network device using the secure communications service via the virtual private network communication link.

2. (Original) The network device of claim 1, wherein:

the secure communications service includes an audio-video conferencing service; and

the at least one processor is configured to execute the secure communications service application program so as to allow the network device to communicate data using the audio-video conferencing service.

3. (Original) The network device of claim 1, wherein the at least one processor is configured to execute the application program so that at least one of video data and audio data can be communicated over the virtual private network communication link using the audio-video conferencing service.

4. (Original) The network device of claim 1, wherein the secure communications service includes a messaging service.

5. (Original) The network device of claim 4, wherein the messaging service includes an e-mail service.

6. (Original) The network device of claim 1, wherein the secure communications service includes a telephony service.

7. (Original) The system of claim 6, wherein the telephony service uses modulation.

8. (Original) The network device of claim 7, wherein the modulation is based on one of frequency-division multiplexing (FDM), time-division multiplexing (TDM), or code division multiple access (CDMA).

9. (Original) The network device of claim 1, wherein the network device is a mobile device.

10. (Original) The network device of claim 9, wherein the mobile device is a notebook computer.

11. (Original) The network device of claim 1, wherein the identifier associated with the second network device is a domain name.

12. (Original) The network device of claim 1, wherein the virtual private network communication link is based on inserting into each data packet communicated over the virtual private network communication link one or more data values that vary according to a pseudo-random sequence.

13. (Original) The network device of claim 1, wherein the virtual private network communication link is based on a network address hopping regime that is used to pseudo-randomly change network addresses in packets transmitted between a first device and a second device.

14. (Original) The network device of claim 1, wherein the indication that the second network device is available for the secure communications service is a function of the result of a domain name lookup.

15. (Original) A method executed by a first network device for communicating with a second network device, the method comprising:

sending a request to look up a network address of a second network device based on an identifier associated with the second network device;

receiving an indication that the second network device is available for a secure communications service, the indication including the requested network address of the second network device and provisioning information for a virtual private network communication link; and

connecting to the second network device over the virtual private network communication link, using the received network address of the second network device and the provisioning information for the virtual private network communication link; and

communicating with the second network device using the secure communications service via the virtual private network communication link.

16. (Original) The method of claim 15, wherein the secure communications service includes a video conferencing service, and communicating includes communicating at least one of video data and audio data using the video conferencing service.

17. (Original) The method of claim 15, further comprising encrypting at least one of the video data and audio data over the virtual private network communication link.

18. (Original) The method of claim 15, wherein the secure communications service includes a messaging service.

19. (Original) The method of claim 18, wherein the messaging service includes an e-mail service.

20. (Original) The method of claim 15, wherein the secure communications service includes a telephony service.

21. (Original) The method of claim 20, wherein the telephony service uses modulation.

22. (Original) The method of claim 21, wherein the modulation is based on one of frequency-division multiplexing (FDM), time-division multiplexing (TDM), or code division multiple access (CDMA).

23. (Original) The method of claim 15, wherein the network device is a mobile device.

24. (Original) The method of claim 23, wherein the mobile device is a notebook computer.

25. (Original) The method of claim 15, wherein the identifier associated with the second network device is a domain name.

26. (Original) The method of claim 15, wherein communicating with the second network device using the secure communications service via the virtual private network communication link includes inserting into data packets communicated over the virtual private network communication link one or more data values that vary according to a pseudo-random sequence.

27. (Original) The method of claim 15, wherein communicating with the second network device using the secure communications service via the virtual private network communication link includes network address hopping regime that is used to pseudorandomly change network addresses in packets transmitted between a first device and a second device.

28. (Original) The method of claim 15, wherein the indication that the second network device is available for a secure communications service is a function of a domain name lookup.

REMARKS

Claims 1-28 are in the application, of which Claims 1 and 15 are the independent claims. Claims 1-28 stand rejected. The rejections are traversed and reconsideration is respectfully requested in view of the following remarks.

Double Patenting Rejections

Claims 1-28 were rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over Claims 1-17 of U.S. Patent No. 6,502,135.

Claims 1-28 were rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over Claims 1, 3-7, 13-16, and 33-40 of U.S. Patent No. 7,188,180.

Claims 1-28 were rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over Claims 1, 8, 9, 12, 13, 14, 16, 17 and 23-33 of U.S. Patent No. 7,418,504.

Claims 1-28 were rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over Claims 1, 8-11, and 14-35 of U.S. Patent No. 7,921,211.

Claims 1-28 were rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over Claims 1-8, 10-13, and 17-18 of U.S. Patent No. 7,987,274.

Claims 1-28 were rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over Claims 1-6, 8-9, and 14-22 of U.S. Patent No. 8,051,181.

Claims 1-28 were provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over Claims 14-20 and 26-39 of U.S. Patent Application No. 13/080,680.

Claims 1-28 were provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over Claims 1-25 of U.S. Patent Application No. 13/336,958.

Claims 1-28 were provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over Claims 1-28 of U.S. Patent Application No. 13/337,757.

Claims 1-28 were provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over Claims 1-28 of U.S. Patent Application No. 13/339,257.

Claims 1-28 were provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over Claims 1-30 of U.S. Patent Application No. 13/342,795.

Claims 1-28 were provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over Claims 1-30 of U.S. Patent Application No. 13/343,465.

In order to expedite prosecution, Terminal Disclaimers are being concurrently herewith. Reconsideration and withdrawal of the rejections are respectfully requested.

Rejections under 35 U.S.C. § 103

Claims 1-28 were rejected under 35 U.S.C. § 103(a) as being unpatentable over the reference, "Windows NT Server, Virtual Private Networking: An Overview" (hereinafter referenced as "*VPN Overview*") and Aventail connect v3.1/v2.6 administrator's Guide References" (hereinafter referenced as "*Aventail*").

- ***Aventail* Has Not Been Shown to Be Prior Art**

Aventail was introduced in a Request for Reexamination of a patent (U.S. Patent No. 6,502,135) owned by the assignee of the instant application. Detailed arguments have been presented in the reexamination proceedings initiated in response to the Request (see Reexamination Control Number 95/001682), detailing the reasons why *Aventail* does not qualify as prior art. The following paragraphs summarize some of the arguments presented in the reexamination proceedings.

M.P.E.P. § 2128 sets forth the requirements for a reference to qualify as a printed publication. Specifically, M.P.E.P. § 2128 provides, in part:

> A reference is a "printed publication" only "upon a satisfactory showing that such document has been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it." *In re Wyer,* 655 F.2d 221, 210 USPQ 790 (C.C.P.A. 1981) (quoting *I.C.E. Corp. v. Armco Steel Corp.*, 250 F. Supp. 738, 743, 148 USPQ 537, 540 (SDNY 1966)).

Therefore, a showing of dissemination and public accessibility are the keys to the legal determination of whether a document was "published."

In the reexamination proceedings, the Requester submitted uncorroborated declarations to support its allegation that *Aventail* qualifies as a "printed publication." However, these declarations are insufficient to establish that *Aventail* is prior art. Specifically, although the declarations state that *Aventail* was distributed with deployments of the Aventail products, no evidence of distribution, not even simply an e-mail from the alleged time period, showing distribution of *Aventail*, has been provided. Further, there is no evidence indicating that *Aventail* was available for download on the Internet in the relevant time period and *Aventail* was not published in any journals.

Applicants respectfully note that the party asserting the prior art bears the burden of establishing a date of publication. *See Carella v. Starlight Archery*, 804 F.2d 135, 139 (Fed. Cir. 1986) (finding that a mailer did not qualify as prior art because there was no evidence as to when the mailer was received by any of the addresses). *See also In re Lister*, 583 F.3d 1307, 1309-17 (Fed. Cir. 2009). However, since there is no evidence of publication of *Aventail*, other than the aforementioned uncorroborated declarations, which were not incorporated or relied on by the Office Action, the logical conclusion is that no evidence of publication exists. As a result, Applicants respectfully submit that each rejection based, in whole or in part, on *Aventail* is fatally defective. Accordingly, Applicants respectfully request that the rejections of Claims 1-28 under 35 U.S.C. § 103(a) be withdrawn.

- ***VPN Overview* Has Not Been Shown to Be Prior Art**

The only indication of time/date in *VPN Overview* is a 1998 copyright year printed on the second page of this reference. However, this copyright date is not *prima facie* evidence of publication. Indeed, *VPN Overview*, on its face, is identified as nothing more than a "draft." (*See VPN Overview*, page 1 (stating "White Paper – DRAFT").) Furthermore, the distinction between a publication date and a copyright date is critical. To establish a date of publication, the reference must be shown to have "been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it." *In re Wyre*, 655 F.2d 221, 226 (C.C.P.A. 1981). Unlike a publication date, a copyright date merely establishes "the date that the document was created or printed" *Hilgraeve, Inc. v. Symantec Corp.*, 271 F. Supp. 2d 964, 975 (E.D. Mich. 2003). A

copyright date of a reference does not in and of itself constitute the date of publication of the reference, and a party asserting the reference as prior art bears the burden of proving when the reference became publicly accessible. *In re Lister*, 583 F.3d 1307, 1309-17 (Fed. Cir. 2009).

Even if the 1998 copyright date of *VPN Overview* is presumed accurate, *VPN Overview's* copyright assertion does not meet the standard of *In re Wyer* and/or *In re Lister*. For example, *VPN Overview's* copyright assertion is not evidence that *Aventail* was "disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it." *See In re Wyer*, 655 F.2d at 226. At best, presuming the author of *VPN Overview* accurately represented its copyright date, this date is merely evidence of a date of creation, **not** of publication or dissemination. Without more, this unsupported assertion of the alleged copyright date of *VPN Overview* as the publication date does not meet the "publication" standard required for a document to be relied upon as prior art. The Office Action failed to provide any evidence that *VPN Overview* was actually distributed and publicly accessible. Therefore, there is no evidence that *VPN Overview* was a printed publication on the date asserted and each rejection based, in whole or in part, on this reference is fatally defective. Accordingly, Applicants respectfully request that the rejections of Claims 1-28 under 35 U.S.C. § 103(a) be withdrawn.

Without admitting that *Aventail* and/or *VPN Overview* were "printed publications" as of the dates asserted, Applicants assume, *arguendo,* that these references are publications as of the asserted dates for the purposes of this response.

- **The 35 U.S.C. § 103(a) Rejections of Claims 1-28 Are Improper and Should Be Withdrawn**

Claim 1 recites:

A network device, comprising:

a storage device storing an application program for a secure communications service; and

at least one processor configured to execute the application program for the secure communications service so as to enable the network device to:

send a request to look up a network address of a second network device based on an identifier associated with the second network device;

receive an indication that the second network device is available for the secure communications service, the indication including the requested network address of the second network device and provisioning information for a virtual private network communication link;

> connect to the second network device, using the received network address of the second network device and the provisioning information for the virtual private network communication link; and
>
> communicate with the second network device using the secure communications service via the virtual private network communication link.

The present Office Action alleges, in part, that independent claims 1 and 15, and certain dependent claims, are disclosed by *Aventail* because *Aventail* discloses:

> A network device comprising the features of:
>
> send a request to look up a network address of a second network device based on an identifier associated with the second network device (*e.g.*, Window TCP/IP network application use WinSock to gain access to networks or the internet … and the application executes a DNS … and requests a connection …, see page 8 of Aventail);
>
> connect to the second network device, using the received network address of the second network device and communicate with the second network device using the secure communications service via the network communication link (*e.g.*, Aventail, Page 77- Depending on the security policy and the Aventail ExtraNet Server configuration, Aventail connect will automatically proxy their allowed application traffic into the private network. In this situation, Aventail connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server. Then, based on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed).

Applicants respectfully submit that, while the Office Action, attempts to link the cited portions of *Aventail* to certain features of claim 1, the Office Action is completely silent as to how *Aventail*, either alone or in combination with any other cited reference, would disclose or make obvious at least the feature of enabling the network device to "receive an indication that the second network device is available for the secure communications service, the indication including the requested network address of the second network device and provisioning information for a virtual private network communication link." Indeed, a review of the cited references reveals that at least this feature is not disclosed or made obvious by the cited references.

Moreover, the Office Action has not provided any reasoning as to how the cited portion of *Aventail*, which discloses that Aventail Connect proxies traffic into the private network "[d]epending on the security policy and the Aventail ExtraNet Server configuration" (*Aventail* at 77), discloses or makes obvious the claimed feature of enabling the network device to "connect

to the second network device, using the received network address of the second network device and the provisioning information for the virtual private network communication link."

VPN Overview is an overview document that provides an overview of Virtual Private Networks, describes their basic requirements, and discusses some of the key technologies that permit private networking over public internetworks (*See VPN Overview*, Abstract). However, *VPN Overview* fails to remedy the previously described deficiencies of *Aventail*.

Accordingly, the Request has not demonstrated, or even properly alleged that *Aventail* or *VPN Overview*, either alone or in combination, discloses or makes obvious the features of Claim 1. "The goal of examination is to clearly articulate any rejection early in the prosecution process so that the applicant has the opportunity to provide evidence of patentability and otherwise reply completely at the earliest opportunity" M.P.E.P. § 706. Indeed, 37 C.F.R. § 1.104 provides that the "pertinence of each reference, if not apparent, must be clearly explained and each rejected claim specified." In the subject rejection, the pertinence of *Aventail* and *VPN Overview* to claim 1 is not apparent from the Office Action. On that basis alone, the rejection of Claim 1 is deficient and should be withdrawn.

Applicants also note that an obviousness rejection requires that "all of the claim limitations [] be taught or suggested by the prior art applied and that all words in a claim must be considered in judging the patentability of that claim against the prior art." *Ex Parte Karl Burgess, David Jones, and Claire Louise Robins*, Appeal 2008-2820, 2009 WL 291172, at *3 (B.P.A.I. Feb. 06, 2009) (citing *In re Wilson*, 424 F.2d 1382, 1385 (CCPA 1970)) (emphasis added). *See also* M.P.E.P. § 2143.03. Since a combination of *Aventail* and *VPN Overview* does not disclose, teach, or suggest at least the feature of "receive an indication that the second network device is available for the secure communications service, the indication including the requested network address of the second network device and provisioning information for a virtual private network communication link," an obviousness rejection of claim 1 based on *Aventail* and *VPN Overview* cannot be maintained.

Accordingly, reconsideration and withdrawal of the rejection of independent Claim 1 are respectfully requested.

Independent Claim 15 is directed, in part, to a method for:

> receiving an indication that the second network device is available for a secure communications service, the indication including the requested network address of the

second network device and provisioning information for a virtual private network communication link; and

connecting to the second network device over the virtual private network communication link, using the received network address of the second network device and the provisioning information for the virtual private network communication link; and

communicating with the second network device using the secure communications service via the virtual private network communication link.

For at least the explanations similar to those described above regarding *Aventail* and *VPN Overview*, Applicants submit that *Aventail* and *VPN Overview*, either alone or in combination, does not disclose or make obvious the features of independent Claim 15. Accordingly, reconsideration and withdrawal of the rejection of independent Claim 15 are respectfully requested.

The other claims currently under consideration in the application are dependent from their respective independent claims discussed above and therefore are believed to be allowable for at least similar reasons. Because each dependent claim is deemed to define an additional aspect of the invention, the individual consideration of each on its own merits is respectfully requested. Reconsideration and withdrawal of the rejections of the dependent claims are respectfully requested.

The absence of a reply to a specific rejection, issue, or comment does not signify agreement with or concession of that rejection, issue, or comment. In addition, because the arguments made above may not be exhaustive, there may be other reasons for patentability of any or all claims that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede, or an actual concession of, any issue with regard to any claim, or any cited art, except as specifically stated in this paper, and the amendment or cancellation of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment or cancellation.

CONCLUSION

In view of the foregoing amendments and remarks, the entire application is believed to be in condition for allowance, and such action is respectfully requested at the Examiner's earliest convenience. Should the Examiner have any questions, please call the undersigned at the phone number listed below.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 502203 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Date: June 1, 2012

/Toby H. Kusmer/
Toby H. Kusmer, P.C., Reg. No. 26,418
Ashley B. Tarokh, Reg. No. 68,651
Customer No. 23630
28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile : (617)535-3800
E-mail: tkusmer@mwe.com

PTO/SB/26 (08-11)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT	Docket Number (Optional) 77580-151 (VRNK-1CP3CNFT1)

In re Application of: Victor Larson, et al.

Application No.: 13/336,790

Filed: December 23, 2011

For: System and Method Employing An Agile Network Protocol for Secure Communications Using Secure Domain Names

The owner*, Virnetx, Inc., of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of **prior patent** No. 7,921,211 as the term of said **prior patent** is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

expires for failure to pay a maintenance fee;
is held unenforceable;
is found invalid by a court of competent jurisdiction;
is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
has all claims canceled by a reexamination certificate;
is reissued; or
is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. ☐ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 47,025

/Toby H. Kusmer/ — Signature
June 1, 2012 — Date

Toby H. Kusmer — Typed or printed name

617.535.4065 — Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/26 (08-11)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT	Docket Number (Optional) 77580-151 (VRNK-1CP3CNFT1)

In re Application of: Victor Larson, et al.

Application No.: 13/336,790

Filed: December 23, 2011

For: System and Method Employing An Agile Network Protocol for Secure Communications Using Secure Domain Names

The owner*, Virnetx, Inc., of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of **prior patent** No. 7,418,504 as the term of said **prior patent** is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

expires for failure to pay a maintenance fee;
is held unenforceable;
is found invalid by a court of competent jurisdiction;
is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
has all claims canceled by a reexamination certificate;
is reissued; or
is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. ☐ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 47,025

/Toby H. Kusmer/ — Signature

June 1, 2012 — Date

Toby H. Kusmer — Typed or printed name

617.535.4065 — Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/25 (08-11)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION

Docket Number (Optional)
77580-151 (VRNK-1CP3CNFT1)

In re Application of: Victor Larson, et al.

Application No.: 13/336,790

Filed: December 23, 2011

For: System and Method Employing an Agile Network Protocol for Secure Communications Using Secure Domain Names

The owner*, Virnetx, Inc., of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending **reference** Application Number 13/337,757, filed December 27, 2011, as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the **reference** application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said **reference** application, "as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application," in the event that: any such patent: granted on the pending **reference** application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

Check either box 1 or 2 below, if appropriate.

1. ☐ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 47,025

/Toby H. Kusmer/ — Signature
June 1, 2012 — Date

Toby H. Kusmer — Typed or printed name

617.535.4065 — Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) is included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this statement. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/25 (08-11)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION

Docket Number (Optional)
77580-151 (VRNK-1CP3CNFT1)

In re Application of: Victor Larson, et al.

Application No.: 13/336,790

Filed: December 23, 2011

For: System and Method Employing an Agile Network Protocol for Secure Communications Using Secure Domain Names

The owner*, Virnetx, Inc., of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending **reference** Application Number 13/342,795, filed January 3, 2012, as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the **reference** application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said **reference** application, "as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application," in the event that: any such patent: granted on the pending **reference** application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

Check either box 1 or 2 below, if appropriate.

1. ☐ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 47,025

/Toby H. Kusmer/ — Signature
June 1, 2012 — Date

Toby H. Kusmer — Typed or printed name

617.535.4065 — Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) is included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this statement. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/25 (08-11)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION

Docket Number (Optional)
77580-151 (VRNK-1CP3CNFT1)

In re Application of: Victor Larson, et al.

Application No.: 13/336,790

Filed: December 23, 2011

For: System and Method Employing an Agile Network Protocol for Secure Communications Using Secure Domain Names

The owner*, Virnetx, Inc., of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending **reference** Application Number 13/080,680, filed April 6, 2011, as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the **reference** application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said **reference** application, "as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application," in the event that: any such patent: granted on the pending **reference** application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

Check either box 1 or 2 below, if appropriate.

1. ☐ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 47,025

/Toby H. Kusmer/ — Signature
June 1, 2012 — Date

Toby H. Kusmer — Typed or printed name

617.535.4065 — Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) is included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this statement. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/26 (08-11)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT

Docket Number (Optional)
77580-151 (VRNK-1CP3CNFT1)

In re Application of: Victor Larson, et al.

Application No.: 13/336,790

Filed: December 23, 2011

For: System and Method Employing An Agile Network Protocol for Secure Communications Using Secure Domain Names

The owner*, Virnetx, Inc., of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of **prior patent** No. 7,188,180 as the term of said **prior patent** is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

expires for failure to pay a maintenance fee;
is held unenforceable;
is found invalid by a court of competent jurisdiction;
is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
has all claims canceled by a reexamination certificate;
is reissued; or
is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. ☐ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 47,025

/Toby H. Kusmer/ — Signature
June 1, 2012 — Date

Toby H. Kusmer — Typed or printed name

617.535.4065 — Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/26 (08-11)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT	Docket Number (Optional) 77580-151 (VRNK-1CP3CNFT1)

In re Application of: Victor Larson, et al.

Application No.: 13/336,790

Filed: December 23, 2011

For: System and Method Employing An Agile Network Protocol for Secure Communications Using Secure Domain Names

The owner*, Virnetx, Inc., of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of **prior patent** No. 8,051,181 as the term of said **prior patent** is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

expires for failure to pay a maintenance fee;
is held unenforceable;
is found invalid by a court of competent jurisdiction;
is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
has all claims canceled by a reexamination certificate;
is reissued; or
is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. ☐ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 47,025

/Toby H. Kusmer/ — Signature
June 1, 2012 — Date

Toby H. Kusmer — Typed or printed name

617.535.4065 — Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/26 (08-11)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT	Docket Number (Optional) 77580-151 (VRNK-1CP3CNFT1)

In re Application of: Victor Larson, et al.

Application No.: 13/336,790

Filed: December 23, 2011

For: System and Method Employing An Agile Network Protocol for Secure Communications Using Secure Domain Names

The owner*, Virnetx, Inc., of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of **prior patent** No. 6,502,135 as the term of said **prior patent** is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

expires for failure to pay a maintenance fee;
is held unenforceable;
is found invalid by a court of competent jurisdiction;
is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
has all claims canceled by a reexamination certificate;
is reissued; or
is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. ☐ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 47,025

/Toby H. Kusmer/ — Signature
June 1, 2012 — Date

Toby H. Kusmer — Typed or printed name

617.535.4065 — Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/25 (08-11)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION

Docket Number (Optional)
77580-151 (VRNK-1CP3CNFT1)

In re Application of: Victor Larson, et al.

Application No.: 13/336,790

Filed: December 23, 2011

For: System and Method Employing an Agile Network Protocol for Secure Communications Using Secure Domain Names

The owner*, Virnetx, Inc., of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending **reference** Application Number 13/339,257, filed December 28, 2011, as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the **reference** application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said **reference** application, "as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application," in the event that: any such patent: granted on the pending **reference** application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

Check either box 1 or 2 below, if appropriate.

1. ☐ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 47,025

/Toby H. Kusmer/ — Signature
June 1, 2012 — Date

Toby H. Kusmer — Typed or printed name

617.535.4065 — Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) is included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this statement. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/26 (08-11)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT	Docket Number (Optional) 77580-151 (VRNK-1CP3CNFT1)

In re Application of: Victor Larson, et al.

Application No.: 13/336,790

Filed: December 23, 2011

For: System and Method Employing An Agile Network Protocol for Secure Communications Using Secure Domain Names

The owner*, Virnetx, Inc., of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of **prior patent** No. 7,987,274 as the term of said **prior patent** is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

expires for failure to pay a maintenance fee;
is held unenforceable;
is found invalid by a court of competent jurisdiction;
is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
has all claims canceled by a reexamination certificate;
is reissued; or
is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. ☐ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 47,025

/Toby H. Kusmer/ — Signature
June 1, 2012 — Date

Toby H. Kusmer — Typed or printed name

617.535.4065 — Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/25 (08-11)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION

Docket Number (Optional)
77580-151 (VRNK-1CP3CNFT1)

In re Application of: Victor Larson, et al.

Application No.: 13/336,790

Filed: December 23, 2011

For: System and Method Employing an Agile Network Protocol for Secure Communications Using Secure Domain Names

The owner*, Virnetx, Inc., of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending **reference** Application Number 13/343,465, filed January 4, 2012, as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the **reference** application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said **reference** application, "as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application," in the event that: any such patent: granted on the pending **reference** application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

Check either box 1 or 2 below, if appropriate.

1. ☐ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 47,025

/Toby H. Kusmer/ — Signature
June 1, 2012 — Date

Toby H. Kusmer — Typed or printed name

617.535.4065 — Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) is included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this statement. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/25 (08-11)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION

Docket Number (Optional)
77580-151 (VRNK-1CP3CNFT1)

In re Application of: Victor Larson, et al.

Application No.: 13/336,790

Filed: December 23, 2011

For: System and Method Employing an Agile Network Protocol for Secure Communications Using Secure Domain Names

The owner*, Virnetx, Inc., of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending **reference** Application Number 13/336,958, filed December 23, 2011, as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the **reference** application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said **reference** application, "as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application," in the event that: any such patent: granted on the pending **reference** application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

Check either box 1 or 2 below, if appropriate.

1. ☐ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 47,025

/Toby H. Kusmer/ — Signature
June 1, 2012 — Date

Toby H. Kusmer — Typed or printed name

617.535.4065 — Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) is included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this statement. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	13336790
Filing Date:	23-Dec-2011
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Toby H. Kusmer./Tricia Tedesco
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Statutory or terminal disclaimer	1814	12	160	1920
		Total in USD ($)		**1920**

Electronic Acknowledgement Receipt

EFS ID:	12915364
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Tricia Tedesco
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	01-JUN-2012
Filing Date:	23-DEC-2011
Time Stamp:	16:48:03
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1920
RAM confirmation Number	3939
Deposit Account	501133
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	ReplyA.pdf	143587 3327aae6b9796a53e0932aee0eb68f13fecc0da0	no	13
Warnings:					
Information:					
2	Terminal Disclaimer Filed	TerminalDisclaimer-135.pdf	374710 668f2a70a3267e7d7522027e8e0ef6fa65d855fe	no	2
Warnings:					
Information:					
3	Terminal Disclaimer Filed	TerminalDisclaimer-180.pdf	374652 f1f7587c92bc6d50aa4c3b869309cc5e27d85e17	no	2
Warnings:					
Information:					
4	Terminal Disclaimer Filed	TerminalDisclaimer-181.pdf	374653 7f942c459d79819b0a109f01d6b9fe509d326fb6	no	2
Warnings:					
Information:					
5	Terminal Disclaimer Filed	TerminalDisclaimer-211.pdf	374653 b8dd94a6194c691a90ea20407b1508643b8b51fe	no	2
Warnings:					
Information:					
6	Terminal Disclaimer Filed	TerminalDisclaimer-257.pdf	343008 658692e13830f8c2a7850e9bc34f77c26fc6bd8c	no	2
Warnings:					
Information:					
7	Terminal Disclaimer Filed	TerminalDisclaimer-274.pdf	374653 0edecd261db9757cbe3e8de4394b7ec22312a1c7	no	2
Warnings:					
Information:					
8	Terminal Disclaimer Filed	TerminalDisclaimer-465.pdf	343007 3f611dc1372ee843d73d5eea28145c0e05ebff3b	no	2

Warnings:					
Information:					
9	Terminal Disclaimer Filed	TerminalDisclaimer-504.pdf	374653 9ea22731cbe9d496c29df06ef9c6b72aa7800ed5	no	2
Warnings:					
Information:					
10	Terminal Disclaimer Filed	TerminalDisclaimer-680.pdf	342989 36aac271a4e89619e86f1ce3fa35b10fb7f3a3d3	no	2
Warnings:					
Information:					
11	Terminal Disclaimer Filed	TerminalDisclaimer-757.pdf	343009 17d96b7e8c38b425f838e9789ed543beb44c6fad	no	2
Warnings:					
Information:					
12	Terminal Disclaimer Filed	TerminalDisclaimer-795.pdf	343005 5223ebfee41e481ce877dc0a66ea0572ddf08ee9	no	2
Warnings:					
Information:					
13	Terminal Disclaimer Filed	TerminalDisclaimer-958.pdf	343007 89f32b5560c2cb54c3429181ce02fae8fe2eef78	no	2
Warnings:					
Information:					
14	Fee Worksheet (SB06)	fee-info.pdf	30622 9ac9f74b7e20d141df50dbff30a67c80f001f30e	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	4480208		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
13/336,790	12/23/2011	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☐ RATE ($)	SMALL ENTITY ☐ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 06/01/2012	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 28	Minus	** 28	= 0	X $ =		OR	X $60=	0
Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $ =		OR	X $250=	0
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	0

AMENDMENT	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/ANTHONY WILLIAMS/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Application Number	Application/Control No.	Applicant(s)/Patent under Reexamination	
	13/336,790	LARSON ET AL.	

Document Code - DISQ	Internal Document – DO NOT MAIL

TERMINAL DISCLAIMER	☒ APPROVED	☐ DISAPPROVED
Date Filed : 06/01/12	This patent is subject to a Terminal Disclaimer	

Approved/Disapproved by:

12 - Tds all approved.

Angie Walker

U.S. Patent and Trademark Office

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/336,790	12/23/2011	Victor Larson	77580-151(VRNK-1CP3CNFT1)	6217

23630 7590 06/14/2012

McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

EXAMINER	
LIM, KRISNA	
ART UNIT	PAPER NUMBER
2453	

NOTIFICATION DATE	DELIVERY MODE
06/14/2012	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mweipdocket@mwe.com

Applicant-Initiated Interview Summary	Application No.	Applicant(s)	
	13/336,790	LARSON ET AL.	
	Examiner	Art Unit	
	KRISNA LIM	2453	

All participants (applicant, applicant's representative, PTO personnel):

(1) *KRISNA LIM*.

(2) *Toby Kusmer* .

(3) *Kenneth Cheney*.

(4) *Ashley Tarokh*.

Date of Interview: *07 June 2012*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1*.

Identification of prior art discussed: *VPN Overview and Aventail*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Counsels discussed the invention and the prior arts and argued that the prior arts did not teach the feature of "receive an indication that the second network device is available for the secure communications service, the indication including the requested network address of the second network device and provisioning information for a secure communication link; and using the indication to connect to the second network device".

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/Krisna Lim/ Primary Examiner, Art Unit 2453	

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Victor Larson *et al.*	:	
Serial No.: 13/336,790	:	Confirmation No. 6217
Filed: December 23, 2011	:	Group Art Unit: 2453
Customer Number: 23630	:	Examiner: Lim, Krisna

For: System and Method Employing an Agile Network Protocol for Secure Communications Using Secure Domain Names

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Interview Summary

Madam,

Applicants thank Examiner Lim for a telephonic interview on June 8, 2012, with Applicants' representatives, Toby Kusmer, Kenneth Cheney, and Ashley Tarokh.

During the interview, the parties discussed the rejections of the independent claims under 35 U.S.C. § 103(a) over *Aventail Connect v3.1/v2.6 Administrator's Guide* (hereinafter referenced as "Aventail") in view of *Windows NT Server, Virtual Private Networking: An Overview* (hereinafter referenced as "VPN Overview"). Applicants' representatives argued that Aventail and VPN Overview fail to teach or suggest receiving "an indication that the second network device is available for the secure communications service, the indication including the requested network address of the second network device and provisioning information for a secure communication link; [and] connect[ing] to the second network device, using the received network address of the second network device," as recited in Applicants' Claim 1.

Applicants are grateful to Examiner Lim for his time and helpful comments.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Date: June 15, 2012

/Toby H. Kusmer/
Toby H. Kusmer, P.C., Reg. No. 26,418
Customer No. 23630
28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile : (617)535-3800
E-mail: tkusmer@mwe.com

Electronic Acknowledgement Receipt

EFS ID:	13025998
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Tricia Tedesco
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	15-JUN-2012
Filing Date:	23-DEC-2011
Time Stamp:	14:23:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	InterviewSummary.pdf	85808 259e3bbf2ce44b0147e45e2b14b46f1061d26fa8	no	2

Warnings:	
Information:	

Total Files Size (in bytes):	85808

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	**13/336,790**
Filing Date	**12-23-2011**
First Named Inventor	**Victor Larson**
Art Unit	**2453**
Examiner Name	**Krisna Lim**
Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes-Number-Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D1208	Cisco Comments and Petition for Reexamination 95/001,679 dated June 14, 2012	
	D1209	Exhibit S, Declaration of Nathaniel Polish, Ph.D.	
	D1210	Exhibit R, Excerpts from Patent Owner & Plaintiff VirnetX Inc.'s First Amended P.R. 3-1 and 3-2 Disclosure of Asserted Claims and Infringement Contentions	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[X] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

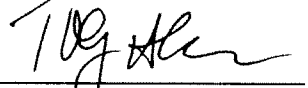
[ ] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.



Date: 6/20/12

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

DM_US 36051951-1.077580.0151

Electronic Acknowledgement Receipt

EFS ID:	13060644
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kerrie Jones
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	20-JUN-2012
Filing Date:	23-DEC-2011
Time Stamp:	14:13:07
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	58364 d7b7f352a566c361d7772ad3bc681cd77e577700	no	2

Warnings:	
Information:	

This is not an USPTO supplied IDS fillable form					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
2	Non Patent Literature	D1208.pdf	3853013 eaf5c634379b23fdc67a94c4331fac1069b67b92	no	69
Warnings:					
Information:					
3	Non Patent Literature	D1209.pdf	239094 bb4f5028b8101ef3fb0a335e73250ba7bfa275c7	no	5
Warnings:					
Information:					
4	Non Patent Literature	D1210.pdf	3178926 9f310e31bbc977b000edec084c28265a8e43fe22	no	53
Warnings:					
Information:					
			Total Files Size (in bytes):	7329397	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	**13/336,790**
Filing Date	**12-23-2011**
First Named Inventor	**Victor Larson**
Art Unit	**2453**
Examiner Name	**Krisna Lim**
Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes-Number-Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D1211	Third Party Requester Comments dated June 25, 2012 - After Non Final Office Action (95/001,788)	
	D1212	Reexam Affidavit/Declaration/Exhibit Filed by 3rd Party on June 25, 2012 (95/001,788)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[X] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[ ] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Date: 6/28/12

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

DM_US 36237561-1.077580.0151

Electronic Acknowledgement Receipt

EFS ID:	13128641
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kerrie Jones
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	28-JUN-2012
Filing Date:	23-DEC-2011
Time Stamp:	12:31:57
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	66755 16f1f6414306b84eeabfc2e902e706c0cb39a6ab	no	2

Warnings:	
Information:	

This is not an USPTO supplied IDS fillable form					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
2	Non Patent Literature	D1211.pdf	1475748 c6b9dbd8510b993a8930b1fdda62698701beec7e	no	37
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
3	Non Patent Literature	D1212.pdf	964426 8301d1b5a831ff5c0e7d4b145f4c91f68810a7bb	no	19
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
Total Files Size (in bytes):			2506929		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	**13/336,790**
Filing Date	**12-23-2011**
First Named Inventor	**Victor Larson**
Art Unit	**2453**
Examiner Name	**Krisna Lim**
Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes-Number-Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D1213	Extended European Search Report dated 03/26/12 from Corresponding European Application Number 11005793.2 (077580-0144)	
	D1214	Bergadano, et al., "Secure WWW Transactions Using Standard HTTP and Java Applets," Proceedings of the 3rd USENIX Workshop on Electronic Commerce, 1998	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[ ] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[X] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Date: 7/24/12

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

DM_US 36887772-1.077580.0151

Electronic Patent Application Fee Transmittal

Application Number:	13336790
Filing Date:	23-Dec-2011
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Hasan M. Rashid/Kerrie Jones
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Electronic Acknowledgement Receipt

EFS ID:	13323301
Application Number:	13336790
International Application Number:	
Confirmation Number:	6217
Title of Invention:	SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Hasan M. Rashid/Kerrie Jones
Filer Authorized By:	Hasan M. Rashid
Attorney Docket Number:	77580-151(VRNK-1CP3CNFT1)
Receipt Date:	24-JUL-2012
Filing Date:	23-DEC-2011
Time Stamp:	12:48:35
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$180
RAM confirmation Number	12809
Deposit Account	501133
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	67075 9fb7c480e1ae5924f2bac5785f18e5c5e681bf14	no	2
Warnings:					
Information:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
This is not an USPTO supplied IDS fillable form					
2	Non Patent Literature	D1213.pdf	136710 74b5ec1dd57786589fb190f9315fb0a9d662ba1e	no	6
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
3	Non Patent Literature	D1214.pdf	484004 e0f438024380229ed5ea85618d3ffd613b7b6488	no	12
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	30669 483b5cc9220c9902c611f5f4476a5b2fe60fc48b	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	718458	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/336,790	12/23/2011	Victor Larson	77580-151(VRNK-1CP3CNFT1)	6217

23630 7590 07/27/2012

McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

EXAMINER	
LIM, KRISNA	
ART UNIT	PAPER NUMBER
2453	

NOTIFICATION DATE	DELIVERY MODE
07/27/2012	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mweipdocket@mwe.com

Office Action Summary	Application No.	Applicant(s)	
	13/336,790	LARSON ET AL.	
	Examiner	Art Unit	
	KRISNA LIM	2453	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 June 2012*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-28* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-28* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

1. Claims 1-28 are still pending for examination.

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained through the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

3. Claims 1-28 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Wesinger [U.S. Patent No. 5,898,830].

4. Wesinger disclosed the invention substantially as claimed. Taking claims 1, 11, 12, 14-15, 26, and 28 as exemplary claims, the reference discloses a network device (i.e., see Internet 120 of Fig. 1 connecting with other network devices), comprising:

a storage device storing an application program for a secure communication service ((i.e., see col. 8 (lines 65) to col. 9 (line 2), col. 16 (line 57) to col. 17 (line 5), col. 12 (lines 23-27)); and

at least one processor configured to execute the application program for the secure communication service so as to enable the network device to:

send a request to look up a network address of a second network device (i.e. a host D) based on an identifier associated with the second network device (i.e., see col. 9, lines 1-25, 53-60);

receive an indication that the second network device is available for the secure communications service, the indication including the requested network address of the second network device and provisioning information for a virtual private network communication link (i.e., see col. 8 (lines 65) to col. 9 (line 2), col. 16 (line 57) to col. 17 (line 5), col. 12 (lines 23-27));

connect to the second network device, using the received network address of the second network device and the provisioning information for the virtual private network communication link (i.e., see col. 8 (lines 65) to col. 9 (line 2), col. 16 (line 57) to col. 17 (line 5), col. 12 (lines 23-27)); and

communicate with the second network device using the secure communications service via the virtual private network communication link (i.e., see col. 8 (lines 65) to col. 9 (line 2), col. 16 (line 57) to col. 17 (line 5), col. 12 (lines 23-27)).

initiating a secure communication link between the first network device (i.e., and the second network device based on a determination that the second network device is available for the secure communications service (i.e., see col. 8 (lines 65) to col. 9 (line 2), col. 16 (line 57) to col. 17 (line 5), col. 12 (lines 23-27));

wherein the secure communication link is a virtual private network communication link and supports data packets (i.e., see col. 12 (lines 23-27) ;

wherein the data is encrypted over the secure communication link (i.e. see col. 12 (lines 23-27) ;

wherein the identifier associated with the second network device is a domain name (i.e., see DNS of Fig. 1, cols. 8 and 9); and

wherein the determining of the second network device is available for a secure communications service is a function of a domain name look up (i.e. see cols. 8 and 9).

5. As to claims 2-10, and 16-24, those features (i.e., video data, audio data, video conference, messaging service, e-mail telephone service using modulation based on FDM, TDM, or CDMA, mobile device, a notebook computer, etc.) are well known the art at the time the invention was made and they are not patentably distinguishable features.

6. As to claims 13 and 27, Wesinger further disclosed the steps of: establishing an IP address hopping scheme between the client and the target (i.e. col. 9, lines 7-25).

7. While Wesinger disclosed, at col. 9 (lines 16-25) the feature of "when a client C tries to initiate a connection to host D using the name D ... The DNS server for D returns the network address of D to a virtual host of the firewall 155. The virtual host returns its network address to the virtual host on the firewall 157 from which it received the lookup request, and so on, until a virtual host on the firewall 105 returns its network address (instead of the network address of D) to the client C", Wesinger did not mention as exactly as the claimed language of “an indication that the second network device is available for the secure communication service, the indication including the requested network address of the second network device and providing information for a virtual private network communication link”. It would have been obvious to one of ordinary skill in the art to obviously recognize that Wesinger’s passage above and the claimed language are obviously the same and the difference is how they are written which is obvious to one of ordinary skill in the art.

A shortened statutory period for response to this action is set to expire 3 (three) months and 0 (zero) days from the mail date of this letter.

Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing

date of this communication.

If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.

Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).

Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Krisna Lim whose telephone number is 571-272-3956 The examiner can normally be reached on Tuesday to Friday from 7:10 AM to 5:40 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Krista Zele, can be reached on 571-272-7288. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free) If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (In USA or Canada) or 571-272-100.

KI
July 20, 2012

/Krisna Lim/

Primary Examiner Art Unit 2453

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes-Number-Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER 'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D1201	Exhibit A-1, Kiuchi[1] vs. Claims of the '135 Patent[2]	
	D1202	Exhibit B-1, Kiuchi[1] vs. Claims of the '211 Patent[2]	
	D1203	Exhibit C-1, Kiuchi[1] vs. Claims of the '504 Patent[2]	
	D1204	Exhibit D, Materials Considered	
	D1205	Exhibit E, Expert Report of Stuart G. Stubblebine, Ph.D.	
	D1206	Exhibit F, Expert Report of Stuart G. Stubblebine, Ph.D.	
	D1207	Exhibit G, Opening Expert Report of Dr. Stuart Stubblebine Regarding Invalidity of the '135, '211, and '504 Patents	

/Krisna Lim/ 07/20/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[X] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[ ] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

/ Toby H. Kusmer /

Date: 6/1/12

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

DM_US 35546776-1.077580.0151

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	**13/336,790**
Filing Date	**12-23-2011**
First Named Inventor	**Victor Larson**
Art Unit	**2453**
Examiner Name	**Krisna Lim**
Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes-Number-Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D1208	Cisco Comments and Petition for Reexamination 95/001,679 dated June 14, 2012	
	D1209	Exhibit S, Declaration of Nathaniel Polish, Ph.D.	
	D1210	Exhibit R, Excerpts from Patent Owner & Plaintiff VirnetX Inc.'s First Amended P.R. 3-1 and 3-2 Disclosure of Asserted Claims and Infringement Contentions	

/Krisna Lim/ 07/20/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** ***(Use as many sheets as necessary)***	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[X] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[ ] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Date: 6/20/12

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

DM_US 36051951-1.077580.0151

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

3-26-12 3/26/12 1FW

Best Available Copy

13336790 - GAU: 2453

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

OPAP IAP23 MAR 23 2012 PATENT & TRADEMARK OFFICE

CERTIFICATION STATEMENT

[X] Under 37 C.F.R. 1.98(d), copies of all patent, publication, pending U.S. application or other information that was previously submitted to, or cited by the USPTO in an earlier application are not required. Applicant will provide copies of the previously submitted references at the Examiner's request. **Enclosed are copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).**

This application claims priority from and is a continuation of a co-pending U.S. Application No. 13/049,552, filed March 16, 2011, which is a continuation of U.S. Application No. 11/840,560, filed August 17, 2007, now U.S. Patent No. 7,921,211, which is a continuation of U.S. Application No. 10/714,849, filed November 18, 2003, now U.S. Patent No. 7,418,504, which is a continuation of U.S. Application No. 09/558,210, filed April 26, 2000, now abandoned, which is a continuation-in-part of U.S. Application No. 09/504,783, filed on February 15, 2000, now U.S. Patent No. 6,502,135, issued December 31, 2002.

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[ ] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[X] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

Date: 3/22/12

03/27/2012 HVUONG1 00000012 501133 13336790
01 FC:1806 180.00 DA

DM_US 32511456-1.077580.0151

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

OPAP
MAR 23 2012
IAP23
PATENT & TRADEMARK OFFICE

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

OPAP
MAR 23 2012
IAP23
PATENT & TRADEMARK OFFICE

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Doc Code: TRAN.LET
Document Description: Transmittal Letter

13336790 - GAU: 2453

PTO/SB/21 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

OPAP
MAR 23 2012
PATENT & TRADEMARK OFFICE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission	52

Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Attorney Docket Number	077580-0151 (VRNK-0001CP3CNFT1)

ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
  - [x] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [x] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [x] Other Enclosure(s) (please Identify below):

Remarks

16 Boxes which include copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	McDermott, Will and Emery		
Signature			
Printed name	Toby H. Kusmer		
Date	March 23, 2012	Reg. No.	26,408

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name		Date	

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

MAR 23 2012 IAP23
PATENT & TRADEMARK OFFICE

PTO/SB/17 (09-11)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

FEE TRANSMITTAL

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Examiner Name	Krisna Lim
Art Unit	2453
Attorney Docket No.	77580-151 VRNK-0001CP3CNFT1

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 180.00

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☑ Deposit Account Deposit Account Number: 50-1133 Deposit Account Name: McDermott, Will and Emery

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☑ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**

☑ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☐ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

Application Type	FILING FEES Fee ($)	FILING FEES Small Entity Fee ($)	SEARCH FEES Fee ($)	SEARCH FEES Small Entity Fee ($)	EXAMINATION FEES Fee ($)	EXAMINATION FEES Small Entity Fee ($)	Fees Paid ($)
Utility	380	190	620	310	250	125	
Design	250	125	120	60	160	80	
Plant	250	125	380	190	200	100	
Reissue	380	190	620	310	750	375	
Provisional	250	125	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	60	30
Each independent claim over 3 (including Reissues)	250	125
Multiple dependent claims	450	225

Total Claims _____ - 20 or HP = _____ x Extra Claims _____ = Fee ($) _____ Fee Paid ($) _____

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims _____ - 3 or HP = _____ x Extra Claims _____ = Fee ($) _____ Fee Paid ($) _____

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims Fee ($) _____ Fee Paid ($) _____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets _____ - 100 = _____ / 50 = _____ (round up to a whole number) x Extra Sheets _____ Fee ($) _____ = Fee Paid ($) _____

4. OTHER FEE(S)

Fees Paid ($)

Non-English Specification, $130 fee (no small entity discount) _____

Other (e.g., late filing surcharge): Information Disclosure Statement Filing Fee $180.00

SUBMITTED BY

Signature		Registration No. (Attorney/Agent) 26,418	Telephone 617-535-4000
Name (Print/Type)	Toby H. Kusmer		Date March 23, 2012

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Applicant: Victor Larson. Docket #. 077580-0151 (VRNK-0001CP3CNFT1

Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES Serial/Reg./Patent No. 13/336,790

Date Sent: March 23, 2012 ☐ Hand Carried ☐ Fax ☐ Electronic ☐ Cert. of Mailing ☒ Express Mail Nos.

EV643771728US
EV643771731US
EV643771743US
EV643771759US
EV643771762US
EV643771776US
EV643771802US
EV643771816US
EV643771780US
EV643771793US

☒ Transmittal Letter

X IDS FORM 1449 (50 pages)

X 16 Boxes of cited references (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).

☒ Fee Transmittal

☐ Response to Missing Parts Notice

☐ Copy of Missing Parts Notice

☐ Replacement Drawing

☐ Maintenance Fee for _____years after grant

☐ Fee Address Indication Form

☐ Terminal Disclaimer

☐ Petition to Commissioner

☐ Status Inquiry

☒ Other RETURN POSTCARD

Check for $	0	☐ Charge Deposit Acct. 50-1133		Atty Init.	THK	Tkpr. #	5470	Secy. or PL:	K. Jones

CMS
Descrip.:

THE PATENT AND TRADEMARK OFFICE DATE STAMPED HEREON IS ACKNOWLEDGEMENT THAT THE ITEMS, CHECKED ABOVE, WERE RECEIVED BY THE PTO ON THE DATE STAMPED.

Accounting

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

3-26-12 3/26/12 13336790 GAU: 2453

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

OPAP IAP23 MAR 23 2012 PATENT & TRADEMARK OFFICE

CERTIFICATION STATEMENT

[X] Under 37 C.F.R. 1.98(d), copies of all patent, publication, pending U.S. application or other information that was previously submitted to, or cited by the USPTO in an earlier application are not required. Applicant will provide copies of the previously submitted references at the Examiner's request. **Enclosed are copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).**

This application claims priority from and is a continuation of a co-pending U.S. Application No. 13/049,552, filed March 16, 2011, which is a continuation of U.S. Application No. 11/840,560, filed August 17, 2007, now U.S. Patent No. 7,921,211, which is a continuation of U.S. Application No. 10/714,849, filed November 18, 2003, now U.S. Patent No. 7,418,504, which is a continuation of U.S. Application No. 09/558,210, filed April 26, 2000, now abandoned, which is a continuation-in-part of U.S. Application No. 09/504,783, filed on February 15, 2000, now U.S. Patent No. 6,502,135, issued December 31, 2002.

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[ ] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[X] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Date: 3/22/12

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

03/27/2012 HVUONG1 00000012 501133 13336790
01 FC:1806 180.00 DA

DM_US 32511456-1.077580.0151

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

OPAP
MAR 23 2012
IAP23
PATENT & TRADEMARK OFFICE

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

OPAP
MAR 23 2012
IAP23
PATENT & TRADEMARK OFFICE

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

EFS Code: TRAN.LET
Document Description: Transmittal Letter

13336790 - GAU: 2453

PTO/SB/21 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

OPAP
MAR 23 2012
PATENT & TRADEMARK OFFICE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission	52

Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Attorney Docket Number	077580-0151 (VRNK-0001CP3CNFT1)

ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
  - [x] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [x] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [x] Other Enclosure(s) (please Identify below):

Remarks

16 Boxes which include copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	McDermott, Will and Emery		
Signature			
Printed name	Toby H. Kusmer		
Date	March 23, 2012	Reg. No.	26,408

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name		Date	

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

PTO/SB/17 (09-11)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

MAR 23 2012 IAP23
PATENT & TRADEMARK OFFICE

FEE TRANSMITTAL

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Examiner Name	Krisna Lim
Art Unit	2453
Attorney Docket No.	77580-151 VRNK-0001CP3CNFT1

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 180.00

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☑ Deposit Account Deposit Account Number: 50-1133 Deposit Account Name: McDermott, Will and Emery

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☑ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**

☑ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☐ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

Application Type	FILING FEES Fee ($)	FILING FEES Small Entity Fee ($)	SEARCH FEES Fee ($)	SEARCH FEES Small Entity Fee ($)	EXAMINATION FEES Fee ($)	EXAMINATION FEES Small Entity Fee ($)	Fees Paid ($)
Utility	380	190	620	310	250	125	
Design	250	125	120	60	160	80	
Plant	250	125	380	190	200	100	
Reissue	380	190	620	310	750	375	
Provisional	250	125	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	60	30
Each independent claim over 3 (including Reissues)	250	125
Multiple dependent claims	450	225

Total Claims _____ - 20 or HP = _____ x Extra Claims _____ = Fee ($) _____ Fee Paid ($) _____

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims _____ - 3 or HP = _____ x Extra Claims _____ = Fee ($) _____ Fee Paid ($) _____

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims Fee ($) _____ Fee Paid ($) _____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets _____ - 100 = _____ / 50 = Extra Sheets _____ (round up to a whole number) x Number of each additional 50 or fraction thereof _____ = Fee ($) _____ Fee Paid ($) _____

4. OTHER FEE(S)

	Fees Paid ($)
Non-English Specification, $130 fee (no small entity discount)	
Other (e.g., late filing surcharge): Information Disclosure Statement Filing Fee	$180.00

SUBMITTED BY

Signature		Registration No. (Attorney/Agent) 26,418	Telephone 617-535-4000
Name (Print/Type)	Toby H. Kusmer		Date March 23, 2012

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Applicant: Victor Larson. Docket #. 077580-0151 (VRNK-0001CP3CNFT1

Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES Serial/Reg./Patent No. 13/336,790

Date Sent: March 23, 2012 ☐ Hand Carried ☐ Fax ☐ Electronic ☐ Cert. of Mailing ☒ Express Mail Nos.

EV643771728US
EV643771731US
EV643771743US
EV643771759US
EV643771762US
EV643771776US
EV643771802US
EV643771816US
EV643771780US
EV643771793US

☒ Transmittal Letter

X IDS FORM 1449 (50 pages)

X 16 Boxes of cited references (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).

☒ Fee Transmittal

☐ Response to Missing Parts Notice

☐ Copy of Missing Parts Notice

☐ Replacement Drawing

☐ Maintenance Fee for ___ years after grant

☐ Fee Address Indication Form

☐ Terminal Disclaimer

☐ Petition to Commissioner

☐ Status Inquiry

☒ Other RETURN POSTCARD

Check for $	0	☐ Charge Deposit Acct. 50-1133		Atty Init.	THK	Tkpr. #	5470	Secy. or PL:	K. Jones

CMS
Descrip.:

THE PATENT AND TRADEMARK OFFICE DATE STAMPED HEREON IS ACKNOWLEDGEMENT THAT THE ITEMS, CHECKED ABOVE, WERE RECEIVED BY THE PTO ON THE DATE STAMPED.

Accounting

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

3/26/12 3-26-12 FW

13336790 GAU: 2453

Subst. for form 1449/RTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

OPAP IAP23 MAR 23 2012 PATENT & TRADEMARK OFFICE

CERTIFICATION STATEMENT

[X] Under 37 C.F.R. 1.98(d), copies of all patent, publication, pending U.S. application or other information that was previously submitted to, or cited by the USPTO in an earlier application are not required. Applicant will provide copies of the previously submitted references at the Examiner's request. **Enclosed are copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).**

This application claims priority from and is a continuation of a co-pending U.S. Application No. 13/049,552, filed March 16, 2011, which is a continuation of U.S. Application No. 11/840,560, filed August 17, 2007, now U.S. Patent No. 7,921,211, which is a continuation of U.S. Application No. 10/714,849, filed November 18, 2003, now U.S. Patent No. 7,418,504, which is a continuation of U.S. Application No. 09/558,210, filed April 26, 2000, now abandoned, which is a continuation-in-part of U.S. Application No. 09/504,783, filed on February 15, 2000, now U.S. Patent No. 6,502,135, issued December 31, 2002.

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[ ] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[X] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Date: 3/22/12

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

03/27/2012 HVUONG1 00000012 501133 13336790
01 FC:1806 180.00 DA

DM_US 32511456-1.077580.0151

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

OPAP
MAR 23 2012
PATENT & TRADEMARK OFFICE
IAP23

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

OPAP IAP23
MAR 23 2012
PATENT & TRADEMARK OFFICE

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record..
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Doc Code: TRAN.LET

Document Description: Transmittal Letter

13336790 - GAU: 2453

PTO/SB/21 (07-09)

Approved for use through 07/31/2012. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

MAR 23 2012 PATENT & TRADEMARK OFFICE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission	52

Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Attorney Docket Number	077580-0151 (VRNK-0001CP3CNFT1)

ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
  - [x] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [x] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [x] Other Enclosure(s) (please Identify below):

Remarks

16 Boxes which include copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	McDermott, Will and Emery		
Signature			
Printed name	Toby H. Kusmer		
Date	March 23, 2012	Reg. No.	26,408

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name		Date	

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

MAR 23 2012 IAP23
PATENT & TRADEMARK OFFICE

PTO/SB/17 (09-11)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

FEE TRANSMITTAL

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Examiner Name	Krisna Lim
Art Unit	2453
Attorney Docket No.	77580-151 VRNK-0001CP3CNFT1

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 180.00

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☑ Deposit Account Deposit Account Number: 50-1133 Deposit Account Name: McDermott, Will and Emery

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☑ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**

☑ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☐ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

Application Type	FILING FEES Fee ($)	FILING FEES Small Entity Fee ($)	SEARCH FEES Fee ($)	SEARCH FEES Small Entity Fee ($)	EXAMINATION FEES Fee ($)	EXAMINATION FEES Small Entity Fee ($)	Fees Paid ($)
Utility	380	190	620	310	250	125	
Design	250	125	120	60	160	80	
Plant	250	125	380	190	200	100	
Reissue	380	190	620	310	750	375	
Provisional	250	125	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	60	30
Each independent claim over 3 (including Reissues)	250	125
Multiple dependent claims	450	225

Total Claims		Extra Claims	Fee ($)		Fee Paid ($)
_____	- 20 or HP =	_____	x _____	=	_____

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims		Extra Claims	Fee ($)		Fee Paid ($)
_____	- 3 or HP =	_____	x _____	=	_____

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims Fee ($)	Fee Paid ($)
_____	_____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets		Extra Sheets		Number of each additional 50 or fraction thereof		Fee ($)		Fee Paid ($)
_____	- 100 =	_____	/ 50 =	_____	(round up to a whole number) x	_____	=	_____

4. OTHER FEE(S)

	Fees Paid ($)
Non-English Specification, $130 fee (no small entity discount)	
Other (e.g., late filing surcharge): Information Disclosure Statement Filing Fee	$180.00

SUBMITTED BY

Signature		Registration No. (Attorney/Agent) 26,418	Telephone 617-535-4000
Name (Print/Type)	Toby H. Kusmer		Date March 23, 2012

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Applicant: Victor Larson. Docket #. 077580-0151 (VRNK-0001CP3CNFT1

Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES Serial/Reg./Patent No. 13/336,790

Date Sent: March 23, 2012 ☐ Hand Carried ☐ Fax ☐ Electronic ☐ Cert. of Mailing ☒ Express Mail Nos.

EV643771728US
EV643771731US
EV643771743US
EV643771759US
EV643771762US
EV643771776US
EV643771802US
EV643771816US
EV643771780US
EV643771793US

☒ Transmittal Letter

X	IDS FORM 1449 (50 pages)	☐	Maintenance Fee for _____years after grant
X	16 Boxes of cited references (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).	☐	Fee Address Indication Form
☒	Fee Transmittal	☐	Terminal Disclaimer
☐	Response to Missing Parts Notice	☐	Petition to Commissioner
☐	Copy of Missing Parts Notice	☐	Status Inquiry
☐	Replacement Drawing	☒	Other RETURN POSTCARD

Check for $	0	☐ Charge Deposit Acct. 50-1133		Atty Init.	THK	Tkpr. #	5470	Secy. or PL:	K. Jones

CMS
Descrip.:

THE PATENT AND TRADEMARK OFFICE DATE STAMPED HEREON IS ACKNOWLEDGEMENT THAT THE ITEMS, CHECKED ABOVE, WERE RECEIVED BY THE PTO ON THE DATE STAMPED.

Accounting

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Best Available Copy

3-26-12

13336790 GAU: 2453

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)

OPAP IAP23 MAR 2 3 2012 PATENT & TRADEMARK OFFICE

CERTIFICATION STATEMENT

[X] Under 37 C.F.R. 1.98(d), copies of all patent, publication, pending U.S. application or other information that was previously submitted to, or cited by the USPTO in an earlier application are not required. Applicant will provide copies of the previously submitted references at the Examiner's request. **Enclosed are copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).**

This application claims priority from and is a continuation of a co-pending U.S. Application No. 13/049,552, filed March 16, 2011, which is a continuation of U.S. Application No. 11/840,560, filed August 17, 2007, now U.S. Patent No. 7,921,211, which is a continuation of U.S. Application No. 10/714,849, filed November 18, 2003, now U.S. Patent No. 7,418,504, which is a continuation of U.S. Application No. 09/558,210, filed April 26, 2000, now abandoned, which is a continuation-in-part of U.S. Application No. 09/504,783, filed on February 15, 2000, now U.S. Patent No. 6,502,135, issued December 31, 2002.

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[ ] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[X] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

Date: 3/22/12

03/27/2012 HVUONG1 00000012 501133 13336790
01 FC:1806 180.00 DA

DM_US 32511456-1.077580.0151

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

OPAP IAP23 MAR 23 2012 PATENT & TRADEMARK OFFICE

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

OPAP IAP23 MAR 23 2012 PATENT & TRADEMARK OFFICE

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Doc Code: TRAN.LET

Document Description: Transmittal Letter

13336790 - GAU: 2453

PTO/SB/21 (07-09)

Approved for use through 07/31/2012. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

O P A P
MAR 23 2012
PATENT & TRADEMARK OFFICE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission	52

Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Attorney Docket Number	077580-0151 (VRNK-0001CP3CNFT1)

ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
  - [x] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [x] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [x] Other Enclosure(s) (please Identify below):

Remarks

16 Boxes which include copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	McDermott, Will and Emery		
Signature			
Printed name	Toby H. Kusmer		
Date	March 23, 2012	Reg. No.	26,408

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name		Date	

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

MAR 23 2012 PATENT & TRADEMARK OFFICE

PTO/SB/17 (09-11)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

FEE TRANSMITTAL

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Examiner Name	Krisna Lim
Art Unit	2453
Attorney Docket No.	77580-151 VRNK-0001CP3CNFT1

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 180.00

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☑ Deposit Account Deposit Account Number: 50-1133 Deposit Account Name: McDermott, Will and Emery

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☑ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, except for the filing fee

☑ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☐ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

Application Type	FILING FEES Fee ($)	FILING FEES Small Entity Fee ($)	SEARCH FEES Fee ($)	SEARCH FEES Small Entity Fee ($)	EXAMINATION FEES Fee ($)	EXAMINATION FEES Small Entity Fee ($)	Fees Paid ($)
Utility	380	190	620	310	250	125	
Design	250	125	120	60	160	80	
Plant	250	125	380	190	200	100	
Reissue	380	190	620	310	750	375	
Provisional	250	125	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	60	30
Each independent claim over 3 (including Reissues)	250	125
Multiple dependent claims	450	225

Total Claims _____ - 20 or HP = _____ x Extra Claims _____ = Fee ($) _____ Fee Paid ($) _____

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims _____ - 3 or HP = _____ x Extra Claims _____ = Fee ($) _____ Fee Paid ($) _____

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims Fee ($) _____ Fee Paid ($) _____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets _____ - 100 = _____ / 50 = _____ (round up to a whole number) x Extra Sheets _____ Number of each additional 50 or fraction thereof Fee ($) _____ = Fee Paid ($) _____

4. OTHER FEE(S)

Fees Paid ($)

Non-English Specification, $130 fee (no small entity discount) _____

Other (e.g., late filing surcharge): Information Disclosure Statement Filing Fee $180.00

SUBMITTED BY

Signature		Registration No. (Attorney/Agent) 26,418	Telephone 617-535-4000
Name (Print/Type)	Toby H. Kusmer		Date March 23, 2012

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Applicant: Victor Larson. Docket #: 077580-0151 (VRNK-0001CP3CNFT1

Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES Serial/Reg./Patent No. 13/336,790

Date Sent: March 23, 2012 ☐ Hand Carried ☐ Fax ☐ Electronic ☐ Cert. of Mailing ☒ Express Mail Nos.

EV643771728US
EV643771731US
EV643771743US
EV643771759US
EV643771762US
EV643771776US
EV643771802US
EV643771816US
EV643771780US
EV643771793US

☒ Transmittal Letter

X	IDS FORM 1449 (50 pages)	☐	Maintenance Fee for _____years after grant
X	16 Boxes of cited references (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).	☐	Fee Address Indication Form
☒	Fee Transmittal	☐	Terminal Disclaimer
☐	Response to Missing Parts Notice	☐	Petition to Commissioner
☐	Copy of Missing Parts Notice	☐	Status Inquiry
☐	Replacement Drawing	☒	Other RETURN POSTCARD

Check for $	0	☐ Charge Deposit Acct. 50-1133		Atty Init.	THK	Tkpr. #	5470	Secy. or PL:	K. Jones

CMS
Descrip.:

THE PATENT AND TRADEMARK OFFICE DATE STAMPED HEREON IS ACKNOWLEDGEMENT THAT THE ITEMS, CHECKED ABOVE, WERE RECEIVED BY THE PTO ON THE DATE STAMPED.

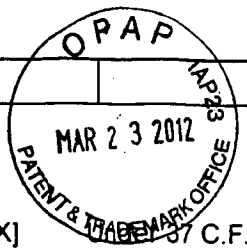
Accounting

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

3/26/12 3-26-12 IFW

13336790 GAU: 2453

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	13/336,790
	Filing Date	12-23-2011
	First Named Inventor	Victor Larson
	Art Unit	2165
	Examiner Name	Krisna Lim
	Docket Number	77580-151(VRNK-0001CP3CNFT1)



CERTIFICATION STATEMENT

[X] Under 37 C.F.R. 1.98(d), copies of all patent, publication, pending U.S. application or other information that was previously submitted to, or cited by the USPTO in an earlier application are not required. Applicant will provide copies of the previously submitted references at the Examiner's request. **Enclosed are copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).**

This application claims priority from and is a continuation of a co-pending U.S. Application No. 13/049,552, filed March 16, 2011, which is a continuation of U.S. Application No. 11/840,560, filed August 17, 2007, now U.S. Patent No. 7,921,211, which is a continuation of U.S. Application No. 10/714,849, filed November 18, 2003, now U.S. Patent No. 7,418,504, which is a continuation of U.S. Application No. 09/558,210, filed April 26, 2000, now abandoned, which is a continuation-in-part of U.S. Application No. 09/504,783, filed on February 15, 2000, now U.S. Patent No. 6,502,135, issued December 31, 2002.

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[ ] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[X] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Date: 3/22/12

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

03/27/2012 HVUONG1 00000012 501133 13336790
01 FC:1806 180.00 DA

DM_US 32511456-1.077580.0151

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

OPAP
MAR 23 2012
IAP23
PATENT & TRADEMARK OFFICE

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

OPAP IAP23
MAR 23 2012
PATENT & TRADEMARK OFFICE

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Doc Code: TRAN.LET

Document Description: Transmittal Letter

13336790 GAU: 2453

PTO/SB/21 (07-09)

Approved for use through 07/31/2012. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

OPAS
MAR 23 2012
PATENT & TRADEMARK OFFICE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Total Number of Pages in This Submission	52
Attorney Docket Number	077580-0151 (VRNK-0001CP3CNFT1)

ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
- [x] Fee Attached
- [ ] Amendment/Reply
- [ ] After Final
- [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [x] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
- [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
- [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [x] Other Enclosure(s) (please Identify below):

Remarks

16 Boxes which include copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	McDermott, Will and Emery		
Signature	/Toby H. Kusmer/		
Printed name	Toby H. Kusmer		
Date	March 23, 2012	Reg. No.	26,408

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name		Date	

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

MAR 23 2012 PATENT & TRADEMARK OFFICE

PTO/SB/17 (09-11)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

FEE TRANSMITTAL

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Examiner Name	Krisna Lim
Art Unit	2453
Attorney Docket No.	77580-151 VRNK-0001CP3CNFT1

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 180.00

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☑ Deposit Account Deposit Account Number: 50-1133 Deposit Account Name: McDermott, Will and Emery

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☑ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**

☑ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☐ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

Application Type	FILING FEES Fee ($)	FILING FEES Small Entity Fee ($)	SEARCH FEES Fee ($)	SEARCH FEES Small Entity Fee ($)	EXAMINATION FEES Fee ($)	EXAMINATION FEES Small Entity Fee ($)	Fees Paid ($)
Utility	380	190	620	310	250	125	
Design	250	125	120	60	160	80	
Plant	250	125	380	190	200	100	
Reissue	380	190	620	310	750	375	
Provisional	250	125	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	60	30
Each independent claim over 3 (including Reissues)	250	125
Multiple dependent claims	450	225

Total Claims _____ - 20 or HP = _____ x Extra Claims _____ Fee ($) _____ = Fee Paid ($) _____

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims _____ - 3 or HP = _____ x Extra Claims _____ Fee ($) _____ = Fee Paid ($) _____

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims Fee ($) _____ Fee Paid ($) _____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets _____ - 100 = _____ / 50 = _____ (round up to a whole number) x Extra Sheets _____ Number of each additional 50 or fraction thereof _____ Fee ($) _____ = Fee Paid ($) _____

4. OTHER FEE(S)

Fees Paid ($)

Non-English Specification, $130 fee (no small entity discount) _____

Other (e.g., late filing surcharge): Information Disclosure Statement Filing Fee $180.00

SUBMITTED BY

Signature		Registration No. (Attorney/Agent) 26,418	Telephone 617-535-4000
Name (Print/Type)	Toby H. Kusmer		Date March 23, 2012

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Applicant: Victor Larson. Docket #. 077580-0151 (VRNK-0001CP3CNFT1

Title: SYSTEM AND METHOD EMPLOYING AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES Serial/Reg./Patent No. 13/336,790

Date Sent: March 23, 2012 ☐ Hand Carried ☐ Fax ☐ Electronic ☐ Cert. of Mailing ☒ Express Mail Nos.

EV643771728US
EV643771731US
EV643771743US
EV643771759US
EV643771762US
EV643771776US
EV643771802US
EV643771816US
EV643771780US
EV643771793US

☒ Transmittal Letter

X	IDS FORM 1449 (50 pages)	☐	Maintenance Fee for ____years after grant
X	16 Boxes of cited references (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).	☐	Fee Address Indication Form
☒	Fee Transmittal	☐	Terminal Disclaimer
☐	Response to Missing Parts Notice	☐	Petition to Commissioner
☐	Copy of Missing Parts Notice	☐	Status Inquiry
☐	Replacement Drawing	☒	Other RETURN POSTCARD

Check for $	0	☐ Charge Deposit Acct. 50-1133		Atty Init.	THK	Tkpr. #	5470	Secy. or PL:	K. Jones

CMS
Descrip.:

THE PATENT AND TRADEMARK OFFICE DATE STAMPED HEREON IS ACKNOWLEDGEMENT THAT THE ITEMS, CHECKED ABOVE, WERE RECEIVED BY THE PTO ON THE DATE STAMPED.

Accounting

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	**13/336,790**
Filing Date	**12-23-2011**
First Named Inventor	**Victor Larson**
Art Unit	**2165**
Examiner Name	**Krisna Lim**
Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A161	6,131,121	10/10/2000	Mattaway et al.	
	A162	6,499,108	12/24/2002	Johnson	

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes-Number-Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	A1112	ITU-T Recommendation H.323, "Infrastructure of Audiovisual Services – Systems and Terminal Equipment for Audiovisual Services. Packet-Based Multimedia Communications System," International Telecommunications Union, pages 1-128, February 1998	
	A1113	ITU-T Recommendation H.225.0, "Infrastructure of Audiovisual Services – Transmission Multiplexing and Synchronization. Call Signaling Protocols and Media Stream Packetization for Packet-Based Multimedia Communication systems," International Telecommunication Union, pages 1-155, February 1998	
	A1114	ITU-T Recommendation H.235, "Infrastructure of Audiovisual Services – Systems Aspects. Security and Encryption for H-Series (H.323 and other H.245-based) Multimedia Terminals," International Telecommunication Union, pages 1-39, February 1998	
	A1115	ITU-T Recommendation H.245, "Infrastructure of Audiovisual Services – Communication Procedures. Control Protocol for Multimedia Communication," International Telecommunication Union, pages 1-280, February 1998	
	A1116	Request for Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No.8,051,181)	
	A1117	Transmittal Letters (Patent No.8,051,181)	
	A1118	Exhibit X5, Droms, R., RFC 2131, "Dynamic Host Configuration Protocol," 1987	

EXAMINER	DATE CONSIDERED
/Krisna Lim/	07/20/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[X] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[ ] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Date: 4/24/12

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

DM_US 33806475-1.077580.0151

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	**13/336,790**
Filing Date	**12-23-2011**
First Named Inventor	**Victor Larson**
Art Unit	**2165**
Examiner Name	**Krisna Lim**
Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes-Number-Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	A1121	Declaration of Angelos D. Keromytis, Ph.D.	
	A1122	Declaration of Dr. Robert Dunham Short III	
	A1123	Exhibit A-1, Verdict Form from VirnetX, Inc. v. Microsoft Corp., No. 6:07-CV-80 (E.D. Tex.)	
	A1124	Exhibit A-3, Declaration of Jason Nieh, Ph.D. (Control No. 95/001,269)	
	A1125	Exhibit A-4, Redacted Deposition of Chris Hopen from VirnetX, Inc. v. Cisco Systems, Inc., No. 6:07-CV 417 (E.D. Tex. April 11, 2012)	
	A1126	Exhibit B-1, Excerpt from Deposition of Defense FY 2000/2001 Biennial Budget Estimates, (Feb. 1999)	
	A1127	Exhibit B-2, Collection of Reports and Presentations on DARPA Projects	
	A1128	Exhibit B-3, Maryann Lawlor, Transient Partnerships Stretch Security Policy Management, Signal Magazine (Sept. 2001) http://www.afcea.org/signal/articles/anmviewer.asp?a=494&print=yes	
	A1129	Joel Snyder, Living in Your Own Private Idaho, Network World (January 28, 1998) http://www.networkworld.com/intranet/0126review.html.	
	A1130	Time Greene, CEO's Chew the VPN Fat, CNN.com (June 17, 1999), http://www.cnn.com/TECH/computing/9906/17/vpnfat.ent.idg/index.html?iref=allsearch	

EXAMINER	/Krisna Lim/	DATE CONSIDERED	07/20/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[X] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[ ] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Date: 5/18/12

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

DM_US 35089818-1.077580.0151

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes–Number 4–Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D1131	Peter Alexander Invalidity Report	
	D1132	Defendants' Second Supplemental Joint Invalidity Contentions	
	D1133	Exhibit 118A, Altiga VPN System[1] vs. Claims of the '135 Patent [2]	
	D1134	Exhibit 119A, Altiga VPN System[1] vs. Claims of the '151 Patent [2]	
	D1135	Exhibit 120A, Altiga VPN System[1] vs. Claims of the '180 Patent [2]	
	D1136	Exhibit 121A, Altiga VPN System[1] vs. Claims of the '211 Patent [2]	
	D1137	Exhibit 122A, Altiga VPN System[1] vs. Claims of the '504 Patent [2]	
	D1138	Exhibit 123A, Altiga VPN System[1] vs. Claims of the '759 Patent [2]	
	D1139	Exhibit 12A, SSL 3.0[1] vs. Claims of the '135 Patent[2]	
	D1140	Exhibit 13A, SSL 3.0[1] vs. Claims of the '504 Patent[2]	
	D1141	Exhibit 14A, SSL 3.0[1] vs. Claims of the '211 Patent[2]	
	D1142	Exhibit 228A, Understanding OSF DCE 1.1 for AIX and OS/2[1] (APP_VX0556531-804) vs. Claims of the '135 Patent[2]	
	D1143	Exhibit 229A, Understanding OSF DCE 1.1 for AIX and OS/2[1] (APP_VX0556531-804) vs. Claims of the '151 Patent[2]	
	D1144	Exhibit 230A, Understanding OSF DCE 1.1 for AIX and OS/2[1] (APP_VX0556531-804) vs. Claims of the '180 Patent[2]	
	D1145	Exhibit 231A, Understanding OSF DCE 1.1 for AIX and OS/2[1] (APP_VX0556531-804) vs. Claims of the '211 Patent[2]	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D1146	Exhibit 232A, Understanding OSF DCE 1.1 for AIX and OS/2[1] (APP_VX0556531-804) vs. Claims of the '504 Patent[2]	
	D1147	Exhibit 233A, Understanding OSF DCE 1.1 for AIX and OS/2[1] (APP_VX0556531-804) vs. Claims of the '759 Patent[2]	
	D1148	Exhibit 255, Schulzrinne[1] vs. Claims of the '135 Patent[2]	
	D1149	Exhibit 256, Schulzrinne[1] vs. Claims of the '504 Patent[2]	
	D1150	Exhibit 257, Schulzrinne[1] vs. Claims of the '211 Patent[2]	
	D1151	Exhibit 258, Schulzrinne[1] vs. Claims of the '151 Patent[2]	
	D1152	Exhibit 259, Schulzrinne[1] vs. Claims of the '180 Patent[2]	
	D1153	Exhibit 260, Schulzrinne[1] vs. Claims of the '759 Patent[2]	
	D1154	Exhibit 261, SSL 3.0[1] vs. Claims of the '151 Patent[2]	
	D1155	Exhibit 262, SSL 3.0[1] vs. Claims of the '759 Patent[2]	
	D1156	Exhibit 263, Wang[1] vs. Claims of the '135 Patent[2]	
	D1157	Wang[1] vs. Claims of the '504 Patent[2]	
	D1158	Wang[1] vs. Claims of the '211 Patent[2]	
	D1159	Exhibit 1, Alexander CV.pdf	
	D1160	Exhibit 2, Materials Considered by Peter Alexander	
	D1161	Exhibit 3, Cross Reference Chart	
	D1162	Exhibit 4, RFC 2543[1] vs. Claims of the '135 Patent	
	D1163	Exhibit 5, RFC 2543[1] vs. Claims of the '504 Patent	
	D1164	Exhibit 6, RFC 2543[1] vs. Claims of the '211 Patent	
	D1165	Exhibit 7, The Schulzrinne Presentation[1] vs. Claims of the '135 Patent	
	D1166	Exhibit 8, The Schulzrinne Presentation[1] vs. Claims of the '504 Patent	
	D1167	Exhibit 9, The Schulzrinne Presentation[1] vs. Claims of the '211 Patent	
	D1168	Exhibit 10, The Schulzrinne Presentation[1] vs. Claims of the '151 Patent	
	D1169	Exhibit 11, The Schulzrinne Presentation[1] vs. Claims of the '180 Patent	
	D1170	Exhibit 12, The Schulzrinne Presentation[1] vs. Claims of the '759 Patent	
	D1171	Exhibit 13, SSL 3.0[2] vs. Claims of the '135 Patent	
	D1172	Exhibit 14, SSL 3.0[2] vs. Claims of the '504 Patent	
	D1173	Exhibit 15, SSL 3.0[2] vs. Claims of the '211 Patent	
	D1174	Exhibit 16, SSL 3.0[2] vs. Claims of the '151 Patent	
	D1175	Exhibit 17, SSL 3.0[2] vs. Claims of the '759 Patent	
	D1176	Exhibit 18, Kiuchi[1] vs. Claims of the '135 Patent	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

	D1177	Exhibit 19, Kiuchi[1] vs. Claims of the '504 Patent	
	D1178	Exhibit 20, Kiuchi[1] vs. Claims of the '211 Patent	
	D1179	Exhibit 21, Kiuchi[1] vs. Claims of the '151 Patent	
	D1180	Exhibit 22, Kiuchi[1] vs. Claims of the '180 Patent	
	D1181	Exhibit 23, Kiuchi[1] vs. Claims of the '759 Patent	
	D1182	Exhibit 24, U.S. Patent No. 6,119,234 (hereinafter "Aziz") and RFC 2401[2] vs. Claims of the '135 Patent	
	D1183	Exhibit 25, U.S. Patent No. 6,119,234 (hereinafter "Aziz") and RFC 2401[2] vs. Claims of the '504 Patent	
	D1184	Exhibit 26, U.S. Patent No. 6,119,234 (hereinafter "Aziz") and RFC 2401[2] vs. Claims of the '211 Patent	
	D1185	Exhibit 27, U.S. Patent No. 6,119,234 (hereinafter "Aziz") and RFC 2401[2] vs. Claims of the '151 Patent	
	D1186	Exhibit 28	
	D1187	Exhibit 29, The Altiga System[1] vs. Claims of the '135 Patent	
	D1188	Exhibit 30, The Altiga System[1] vs. Claims of the '504 Patent	
	D1189	Exhibit 31, The Altiga System[1] vs. Claims of the '211 Patent	
	D1190	Exhibit 32, The Altiga System[1] vs. Claims of the '759 Patent	
	D1191	Exhibit 33, U.S. Patent No. 6,496,867 ("Beser")[1]and RFC 2401[2] vs. Claims of the '135 Patent	
	D1192	Exhibit 34, U.S. Patent No. 6,496,867 ("Beser")[1]and RFC 2401[2] vs. Claims of the '504 Patent	
	D1193	Exhibit 35, U.S. Patent No. 6,496,867 ("Beser")[1]and RFC 2401[2] vs. Claims of the '211 Patent	
	D1194	Exhibit 36, U.S. Patent No. 6,496,867 ("Beser")[1]and RFC 2401[2] vs. Claims of the '151 Patent	
	D1195	Exhibit 37, U.S. Patent No. 6,496,867 ("Beser")[1]and RFC 2401[2] vs. Claims of the '180 Patent	
	D1196	Exhibit 38, Kent[1] vs. Claims of the '759 Patent	
	D1197	Exhibit 39, RFC 2538, Storing Certificates in the Domain Name System (DNS)[1] vs. Claims of the '504 Patent[2]	
	D1198	Exhibit 40, RFC 2538, Storing Certificates in the Domain Name System (DNS)[1] vs. Claims of the '211 Patent[2]	
	D1199	Exhibit 41, Aziz ('646)[1] vs. Claims of the '759 Patent	
	D1200	Exhibit 42, The PIX Firewall[1] vs. Claims of the '759 Patent	

EXAMINER	DATE CONSIDERED
/Krisna Lim/	07/20/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[X] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[ ] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Toby H. Kusmer

Date: 6/1/12

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

DM_US 35497951-1.077580.0151

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13336790	LARSON ET AL.
	Examiner	**Art Unit**
	KRISNA LIM	2453

SEARCHED			
Class	**Subclass**	**Date**	**Examiner**
709	223-227	02/23/2012	kl
	updated above	07/20/2012	kl

SEARCH NOTES		
Search Notes	**Date**	**Examiner**
East, Inventors	02/23/2012	kl

INTERFERENCE SEARCH			
Class	**Subclass**	**Date**	**Examiner**

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	**13/336,790**
Filing Date	**12-23-2011**
First Named Inventor	**Victor Larson**
Art Unit	**2453**
Examiner Name	**Krisna Lim**
Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes-Number-Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D1211	Third Party Requester Comments dated June 25, 2012 - After Non Final Office Action (95/001,788)	
	D1212	Reexam Affidavit/Declaration/Exhibit Filed by 3rd Party on June 25, 2012 (95/001,788)	

EXAMINER	/Krisna Lim/	DATE CONSIDERED	07/20/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** ***(Use as many sheets as necessary)***	**Complete if Known**	
	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[X] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[ ] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

Date: 6/28/12

DM_US 36237561-1.077580.0151

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13336790	LARSON ET AL.
	Examiner	**Art Unit**
	KRISNA LIM	2453

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	02/25/2012	07/20/2012							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	✓							
	11	✓	✓							
	12	✓	✓							
	13	✓	✓							
	14	✓	✓							
	15	✓	✓							
	16	✓	✓							
	17	✓	✓							
	18	✓	✓							
	19	✓	✓							
	20	✓	✓							
	21	✓	✓							
	22	✓	✓							
	23	✓	✓							
	24	✓	✓							
	25	✓	✓							
	26	✓	✓							
	27	✓	✓							
	28	✓	✓							

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	**13/336,790**
Filing Date	**12-23-2011**
First Named Inventor	**Victor Larson**
Art Unit	**2165**
Examiner Name	**Krisna Lim**
Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes-Number-Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	A1119	Hopen Transcript dated April 11, 2012	
	A1120	VirnetX Claim Construction Opinion	

EXAMINER	DATE CONSIDERED
/Krisna Lim/	07/20/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

CERTIFICATION STATEMENT

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[X] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[ ] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Toby H. Kusmer, Reg. No. 46,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

Date: May 3, 2012

DM_US 34023885-1.077580.0151

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

3-26-12

13336790 - GAU 2453

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/336,790**
	Filing Date	**12-23-2011**
	First Named Inventor	**Victor Larson**
	Art Unit	**2165**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-151(VRNK-0001CP3CNFT1)**

OPAP IAP23 MAR 23 2012 PATENT & TRADEMARK OFFICE

CERTIFICATION STATEMENT

[X] Under 37 C.F.R. 1.98(d), copies of all patent, publication, pending U.S. application or other information that was previously submitted to, or cited by the USPTO in an earlier application are not required. Applicant will provide copies of the previously submitted references at the Examiner's request. **Enclosed are copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).**

This application claims priority from and is a continuation of a co-pending U.S. Application No. 13/049,552, filed March 16, 2011, which is a continuation of U.S. Application No. 11/840,560, filed August 17, 2007, now U.S. Patent No. 7,921,211, which is a continuation of U.S. Application No. 10/714,849, filed November 18, 2003, now U.S. Patent No. 7,418,504, which is a continuation of U.S. Application No. 09/558,210, filed April 26, 2000, now abandoned, which is a continuation-in-part of U.S. Application No. 09/504,783, filed on February 15, 2000, now U.S. Patent No. 6,502,135, issued December 31, 2002.

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[ ] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[X] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Date: 3/22/12

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

03/27/2012 HVUONG1 00000012 501133 13336790
01 FC:1806 180.00 DA

DM_US 32511456-1.077580.0151

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

OPAP
MAR 2 3 2012
IAP23
PATENT & TRADEMARK OFFICE

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

OPAP IAP23 MAR 23 2012 PATENT & TRADEMARK OFFICE

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Doc Code: TRAN.LET
Document Description: Transmittal Letter

13336790 - GAU: 2453

OPAP 12-23
MAR 2 3 2012
PATENT & TRADEMARK OFFICE

PTO/SB/21 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Attorney Docket Number	077580-0151 (VRNK-0001CP3CNFT1)

Total Number of Pages in This Submission: 52

ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
  - [x] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [x] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [x] Other Enclosure(s) (please Identify below):

Remarks

16 Boxes which include copies of references not previously submitted in a priority application (C8, C19, C21, C24; D257, D258, D261, D263, D264, D266, D292-D1111).

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	McDermott, Will and Emery		
Signature	[signature]		
Printed name	Toby H. Kusmer		
Date	March 23, 2012	Reg. No.	26,408

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name		Date	

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

OPAP IAP23 MAR 23 2012 PATENT & TRADEMARK OFFICE

Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

FEE TRANSMITTAL

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 180.00

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Examiner Name	Krisna Lim
Art Unit	2453
Attorney Docket No.	77580-151 VRNK-0001CP3CNFT1

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☑ Deposit Account Deposit Account Number: 50-1133 Deposit Account Name: McDermott, Will and Emery

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☑ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**

☑ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☐ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

Application Type	FILING FEES Fee ($)	FILING FEES Small Entity Fee ($)	SEARCH FEES Fee ($)	SEARCH FEES Small Entity Fee ($)	EXAMINATION FEES Fee ($)	EXAMINATION FEES Small Entity Fee ($)	Fees Paid ($)
Utility	380	190	620	310	250	125	
Design	250	125	120	60	160	80	
Plant	250	125	380	190	200	100	
Reissue	380	190	620	310	750	375	
Provisional	250	125	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	60	30
Each independent claim over 3 (including Reissues)	250	125
Multiple dependent claims	450	225

Total Claims _____ - 20 or HP = _____ x _____ = _____ Extra Claims / Fee ($) / Fee Paid ($)

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims _____ - 3 or HP = _____ x _____ = _____ Extra Claims / Fee ($) / Fee Paid ($)

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims Fee ($) _____ Fee Paid ($) _____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets _____ - 100 = _____ Extra Sheets / 50 = _____ Number of each additional 50 or fraction thereof (round up to a whole number) x _____ Fee ($) = _____ Fee Paid ($)

4. OTHER FEE(S)

Non-English Specification, $130 fee (no small entity discount) Fees Paid ($) _____

Other (e.g., late filing surcharge): Information Disclosure Statement Filing Fee $180.00

SUBMITTED BY

Signature		Registration No. (Attorney/Agent) 26,418	Telephone 617-535-4000
Name (Print/Type)	Toby H. Kusmer		Date March 23, 2012

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

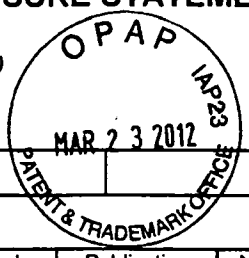
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)



Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

13936790 - GAU: 2453

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Patent Number	Patent Date	Inventor	
	A1	09/399,753	09/22/1998	Graig Miller et al.	
	A2	2,895,502	07/21/1959	Roper et al.	
	A3	4,761,334	08/1988	Sagoi et al.	
	A4	4,885,778	12/5/1989	Weiss, Kenneth	
	A5	4,920,484	4/24/1990	Ranade	
	A6	4,933,846	06/12/1990	Humphrey et al.	
	A7	4,952,930	08/28/1990	Franaszek et al.	
	A8	4,988,990	01/29/1991	Warrior	
	A9	5,164,988	11/17/1992	Matyas	
	A10	5,204,961	04/20/1993	Barlow	
	A11	5,276,735	01/04/1994	Boebert et al	
	A12	5,303,302	04/12/1994	Burrows	
	A13	5,311,593	05/10/1994	Carmi	
	A14	5,329,521	07/12/1994	Walsh et al.	
	A15	5,341,426	08/23/1994	Barney et al.	
	A16	5,367,643	11/22/1994	Chang et al	
	A17	5,384,848	01/24/1995	Kikuchi	
	A18	5,511,122	04/23/1996	Atkinson	
	A19	5,548,646	08/20/1996	Aziz et al.	
	A20	5,559,883	09/24/1996	Williams	
	A21	5,561,669	10/01/1996	Lenney et al	
	A22	5,588,060	12/24/1996	Aziz	
	A23	5,590,285	12/31/1996	Krause et al.	
	A24	5,625,626	04/29/1997	Umekita	
	A25	5,629,984	05/13/1997	McManis	
	A26	5,654,695	08/05/1997	Olnowich et al	
	A27	5,682,480	10/28/1997	Nakagawa	
	A28	5,689,566	11/18/1997	Nguyen	
	A29	5,689,641	11/18/1997	Ludwig et al.	
	A30	5,740,375	04/14/1998	Dunne et al.	
	A31	5,757,925	05/1998	Faybishenko	
	A32	5,764,906	06/1998	Edelstein et al.	
	A33	5,771,239	06/23/1998	Moroney et al.	
	A34	5,774,660	6/30/1998	Brendel et al	
	A35	5,787,172	07/28/1998	Arnold	
	A36	5,790,548	08/04/1998	Sitaraman et al.	
	A37	5,796,942	08/18/1998	Esbensen	
	A38	5,805,801	09/08/1998	Holloway et al.	
	A39	5,805,803	09/08/1998	Birrell et al.	
	A40	5,822,434	10/13/1998	Caronni et al.	
	A41	5,842,040	11/24/1998	Hughes et al.	
	A42	5,845,091	12/01/1998	Dunne et al.	
	A43	5,864,666	01/1999	Shrader, Theodore Jack London	
	A44	5,867,650	02/02/1998	Osterman	
	A45	5,870,610	02/09/1999	Beyda et al.	
	A46	5,878,231	05/02/1999	Baehr et al	
	A47	5,892,903	04/06/1999	Klaus	
	A48	5,898,830	04/27/1999	Wesinger, Jr. et al.	
	A49	5,905,859	05/18/1999	Holloway et al.	
	A50	5,918,018	06/29/1999	Gooderum et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

/Krisna Lim/ 07/20/2012

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

	A51		5,918,019	06/29/1999	Valencia	
	A52		5,950,195	09/07/1999	Stockwell et al.	
	A53		5,950,519	09/14/1999	Anatoli	
	A54		5,960,204	09/28/1999	Yinger et al.	
	A55		5,996,016	11/30/1999	Thalheimer et al.	
	A56		6,006,259	12/21/1999	Adelman et al.	
	A57		6,006,272	12/21/1999	Aravamudan et al	
	A58		6,016,318	01/18/2000	Tomoike	
	A59		6,016,512	01/18/2000	Huitema	
	A60		6,041,342	03/21/2000	Yamaguchi	
	A61		6,052,788	04/2000	Wesinger et al.	
	A62		6,055,574	04/25/2000	Smorodinsky et al.	
	A63		6,061,346	05/2000	Nordman, Mikael	
	A64		6,061,736	05/09/2000	Rochberger et al	
	A65		6,079,020	06/20/2000	Liu	
	A66		6,081,900	06/2000	Subramaniam et al.	
	A67		6,092,200	07/18/2000	Muniyappa et al.	
	A68		6,101,182	08/2000	Sistanizadeh et al.	
	A69		6,119,171	09/12/2000	Alkhatib	
	A70		6,119,234	09/12/2000	Aziz et al.	
	A71		6,147,976	11/14/2000	Shand et al.	
	A72		6,157,957	12/05/2000	Berthaud	
	A73		6,158,011	12/05/2000	Chen et al.	
	A74		6,168,409	01/02/2001	Fare	
	A75		6,173,399	01/09/2001	Gilbrech	
	A76		6,175,867	01/16/2001	Taghadoss	
	A77		6,178,409	01/23/2001	Weber et al.	
	A78		6,178,505	01/23/2001	Schneider et al	
	A79		6,179,102	01/30/2001	Weber, et al.	
	A80		6,182,141	1/30/2001	Blum et al.	
	A81		6,199,112	03/2001	Wilson, Stephen K.	
	A82		6,202,081	03/2001	Naudus, Stanley T.	
	A83		6,222,842	04/24/2001	Sasyan et al.	
	A84		6,223,287	04/24/2001	Douglas et al.	
	A85		6,226,748	05/01/2001	Bots et al.	
	A86		6,226,751	05/01/2001	Arrow et al..	
	A87		6,233,618	05/15/2001	Shannon	
	A88		6,243,360	06/05/2001	Basilico	
	A89		6,243,749	06/05/2001	Sitaraman et al.	
	A90		6,243,754	06/05/2001	Guerin et al	
	A91		6,246,670	06/12/2001	Karlsson et al.	
	A92		6,256,671	07/03/2001	Strentzsch et al.	
	A93		6,262,987	07/17/01	Mogul, Jeffrey C.	
	A94		6,263,445	07/17/2001	Blumenau	
	A95		6,269,099	07/31/2001	Borella et al.	
	A96		6,286,047	09/04/2001	Ramanathan et al	
	A97		6,298,341	10/02/01	Mann, et al.	
	A98		6,301,223	10/9/2001	Hrastar et al	
	A99		6,308,213	10/23/2001	Valencia	
	A100		6,308,274	10/23/2001	Swift	
	A101		6,311,207	10/30/2001	Mighdoll et al	
	A102		6,314,463	11/2001	Abbott et al.	
	A103		6,324,161	11/27/2001	Kirch	
	A104		6,330,562	12/11/2001	Boden et al.	
	A105		6,332,158	12/18/2001	Risley et al.	
	A106		6,333,272	12/25/01	McMillin, et al.	
	A107		6,338,082	01/08/02	Schneider, Eric	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

/Krisna Lim/ 07/20/2012

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

	A108		6,353,614	03/05/2002	Borella et al.	
	A109		6,425,003	07/23/2002	Herzog et al.	
	A110		6,430,155	08/06/2002	Davie et al	
	A111		6,430,610	08/06/2002	Carter	
	A112		6,487,598	11/26/2002	Valencia	
	A113		6,496,867	12/17/2002	Beser et al.	
	A114		6,502,135	12/2002	Munger et al.	
	A115		6,505,232	01/07/2003	Mighdoll et al	
	A116		6,510,154	01/21/2003	Mayes et al	
	A117		6,549,516	04/15/2003	Albert et al	
	A118		6,557,037	04/2003	Provino, Joseph E.	
	A119		6,560,634	05/06/2003	Broadhurst	
	A120		6,571,296	05/27/2002	Dillon	
	A121		6,571,338	05/27/2003	Shaio et al.	
	A122		6,581,166	7/17/2003	Hirst et al.	
	A123		6,606,708	08/12/2003	Devine et al.	
	A124		6,615,357	9/2/2003	Boden et al.	
	A125		6,618,761	09/09/2003	Munger et al.	
	A126		6,671,702	12/30/2003	Kruglikov et al	
	A127		6,687,551	2/3/2004	Steindl	
	A128		6,687,746	02/03/04	Shuster, et al.	
	A129		6,701,437	03/02/2004	Hoke et al.	
	A130		6,714,970	3/30/2004	Fiveash et al.	
	A131		6,717,949	4/6/2004	Boden et al.	
	A132		6,751,738	06/15/2004	Wesinger, Jr. et al..	
	A133		6,752,166	06/22/04	Lull, et al.	
	A134		6,757,740	06/29/04	Parekh, et al.	
	A135		6,760,766	7/6/2004	Sahlqvist	
	A136		6,813,777	11/2004	Weinberger et al.	
	A137		6,826,616	11/30/2004	Larson et al.	
	A138		6,839,759	1/4/2005	Larson et al.	
	A139		6,937,597	08/30/2005	Rosenberg et al.	
	A140		60/134,547	05/17/1999	Victory Sheymov	
	A141		60/151,563	08/31/1999	Bryan Whittles	
	A142		7,010,604	3/7/2006	Munger et al.	
	A143		7,039,713	05/2006	Van Gunter et al.	
	A144		7,072,964	07/04/2006	Whittle et al.	
	A145		7,133,930	11/7/2006	Munger et al.	
	A146		7,167,904	01/23/07	Devarajan, et al.	
	A147		7,188,175	03/06/07	McKeeth, James A.	
	A148		7,188,180	3/6/2007	Larson et al.	
	A149		7,197,563	3/27/2007	Sheymov et al.	
	A150		7,353,841	04/08/08	Kono, et al.	
	A151		7,418,504	08/2008	Larson et al.	
	A152		7,461,334	12/02/08	Lu, et al.	
	A153		7,490,151	02/2009	Munger et al.	
	A154		7,493,403	02/2009	Shull et al.	
	A155		7,584,500	09/2009	Dillon et al.	
	A156		7,764,231	07/27/2010	Karr et al.	
	A157		7,852,861	12/2010	Wu et al.	
	A158		7,921,211	04/2011	Larson et al.	
	A159		7,933,990	04/2011	Munger et al.	
	A160		8,051,181	11/2011	Larson et al.	

/Krisna Lim/ 07/20/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	B1	US2001/0049741	12/2001	Skene et al.	
	B2	US2002/0004898	1/10/02	Droge	
	B3	US2003/0196122	10/16/2003	Wesinger, Jr. et al.	
	B4	US2004/0199493	10/2004	Ruiz et al.	
	B5	US2004/0199520	10/2004	Ruiz et al.	
	B6	US2004/0199608	10/2004	Rechterman et al.	
	B7	US2004/0199620	10/2004	Ruiz et al.	
	B8	US2005/0055306	3/10/05	Miller et al.	
	B9	US2005/0108517	05/2005	Dillon et al.	
	B10	US2006/0059337	03/16/2006	Polyhonen et al.	
	B11	US2006/0123134	06/2006	Munger et al.	
	B12	US2007/0208869	09/2007	Adelman et al.	
	B13	US2007/0214284	09/2007	King et al.	
	B14	US2007/0266141	11/2007	Norton, Michael Anthony	
	B15	US2008/0005792	01/2008	*Larson et al.	
	B16	US2008/0144625	06/2008	Wu et al.	
	B17	US2008/0235507	09/2008	Ishikawa et al.	
	B18	US2009/0193498	07/2009	Agarwal et al.	
	B19	US2009/0193513	07/2009	Agarwal et al.	
	B20	US2009/0199258	08/2009	Deng et al.	
	B21	US2009/0199285	09/2009	Agarwal et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3 – Number 4 –Kind Code5 (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No
	C1	DE19924575	12/2/99	Provino et al.			
	C2	EP0814589	12/29/1997	AT&T Corp.			
	C3	EP0838930	4/29/1988	Digital Equipment Corporation			
	C4	EP0858189	8/12/98	Maciel et al.			
	C5	EP836306	4/15/1998	HEWLETT PACKARD CO			
	C6	GB2317792	04/01/1998	Secure Computing Corporation			
	C7	GB2334181	08/11/1999	NEC Technologies			
	C8	GB2340702	02/23/2000	Sun Microsystems Inc.			
	C9	JP04-363941	12/16/1992	Nippon Telegr & Teleph Corp			
	C10	JP09-018492	01/17/1997	Nippon Telegr & Teleph Corp			
	C11	JP10-070531	03/10/1998	Brother Ind Ltd.			
	C12	JP62-214744	9/21/1987	Hitachi Ltd.			
	C13	WO0070458	11/23/2000	Comsec Corporation			
	C14	WO0017775	3/30/00	Miller et al.			
	C15	WO01016766	03/08/2001	Science Applications International Corporation			
	C16	WO0150688	7/12/01	Kriens			
	C17	WO9827783	06/25/1998	Northern Telecom Limited			
	C18	WO9855930	12/10/98	Tang			

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

/Krisna Lim/ 7/12/2012

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

	C19	WO9843396	10/01/1998	Northern Telecom Limited			
	C20	WO9859470	12/30/98	Kanter et al.			
	C21	WO9911019	03/04/1999	V One Corp			
	C22	WO9938081	7/29/99	Paulsen et al.			
	C23	WO9948303	9/23/99	Cox et al.			
	C24	WO01/61922	02/12/2001	Science Application International Corporation			

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D1	Alan 0. Frier et al., "The SSL Protocol Version 3.0", Nov. 18, 1996, printed from http://www.netscape.com/eng/ss13/ draft302.txt on Feb. 4, 2002, 56 pages.	
	D2	August Bequai, "Balancing Legal Concerns Over Crime and Security in Cyberspace", Computer & Security, vol. 17, No. 4, 1998, pp. 293-298.	
	D3	D. B. Chapman et al., "Building Internet Firewalls", Nov. 1995, pp. 278-375.	
	D4	D. Clark, "US Calls for Private Domain-Name System", Computer, IEEE Computer Society, Aug. 1, 1998, pp. 22-25.	
	D5	Davila J et al, "Implementation of Virtual Private Networks at the Transport Layer", Information Security, Second International Work-shop, ISW'99. Proceedings (Lecture Springer-Verlag Berlin, Germany, [Online] 1999, pp. 85-102, XP002399276, ISBN 3-540-666	
	D6	Dolev, Shlomi and Ostrovsky, Rafil, "Efficient Anonymous Multicast and Reception" (Extended Abstract), 16 pages.	
	D7	Donald E. Eastlake, 3rd, "Domain Name System Security Extensions", INTERNET DRAFT, Apr. 1998, pp. 1-51.	
	D8	F. Halsall, "Data Communications, Computer Networks and Open Systems", Chapter 4, Protocol Basics, 1996, pp. 198-203.	
	D9	Glossary for the Linux FreeS/WAN project, printed from http://liberty.freeswan.org/freeswan_trees/freeswan-1.3/ doc/glossary.html on Feb. 21, 2002, 25 pages.	
	D10	J. Gilmore, "Swan: Securing the Internet against Wiretapping", printed from http://liberty.freeswan.org/freeswan _trees/freeswan-1.3/doc/rationale.html on Feb. 21, 2002, 4 pages.	
	D11	James E. Bellaire, "New Statement of Rules-Naming Internet Domains", Internet Newsgroup, Jul. 30, 1995, 1 page.	
	D12	Jim Jones et al., "Distributed Denial of Service Attacks: Defenses", Global Integrity Corporation, 2000, pp. 1-14.	
	D13	Laurie Wells (LANCASTERBIBELMAIL MSN COM); "Subject: Security Icon" USENET Newsgroup, Oct. 19, 1998, XP002200606, 1 page.	
	D14	Linux FreeS/WAN Index File, printed from http://liberty.freewan.org/freeswan_trees/freeswan-1.3/doc/ on Feb. 21, 2002, 3 Pages.	
	D15	P. Srisuresh et al., "DNS extensions to Network address Translators (DNS_ALG)", Internet Draft, Jul. 1998, pp. 1-27.	
	D16	Reiter, Michael K. and Rubin, Aviel D. (AT&T Labs-Research), "Crowds: Anonymity for Web Transactions", pp. 1-23.	
	D17	RFC 2401 (dated Nov. 1998) Security Architecture for the Internet Protocol (RTP)	
	D18	RFC 2543-SIP (dated March 1999): Session Initiation Protocol (SIP or SIPS)	
	D19	Rich Winkel, "CAQ: Networking With Spooks: The NET & The Control Of Information", Internet Newsgroup, Jun. 21, 1997, 4 pages.	
	D20	Rubin, Aviel D., Geer, Daniel, and Ranum, Marcus J. (Wiley Computer Publishing), "Web Security Sourcebook", pp. 82-94.	
	D21	Search Report (dated Aug. 20, 2002), International Application No. PCT/US01/04340.	
	D22	Search Report (dated Aug. 23, 2002), International Application No. PCT/US01/13260.	
	D23	Search Report (dated Oct. 7, 2002), International Application No. PCT/US01/13261.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

/Krisna Lim/ 12/20/2012

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

	D24	Search Report, IPER (dated Nov. 13, 2002), International Application No. PCT/US01/04340.	
	D25	Search Report, IPER (dated Feb. 06, 2002), International Application No. PCT/US01/13261.	
	D26	Search Report, IPER (dated Jan. 14, 2003), International Application No. PCT/US01/13260.	
	D27	Shankar, A.U. "A verified sliding window protocol with variable flow control". Proceedings of ACM SIGCOMM conference on Communications architectures & protocols. pp. 84-91, ACM Press, NY, NY 1986.	
	D28	Shree Murthy et al., "Congestion-Oriented Shortest Multi-path Routing", Proceedings of IEEE INFOCOM, 1996, pp. 1028-1036.	
	D29	W. Stallings, "Cryptography And Network Security", 2nd, Edition, Chapter 13, IP Security, Jun. 8, 1998, pp. 399-440.	
	D30	Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009, VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation.	
	D31	Appendix A of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	D32	Concordance Table For the References Cited in Tables on pages 6-15, 71-80 and 116-124 of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	D33	1. P. Mockapetris, "DNS Encoding of Network Names and Other Types," Network Working Group, RFC 1101 (April 1989) RFC1101, DNS SRV)	
	D34	R. Atkinson, "An Internetwork Authentication Architecture," Naval Research Laboratory, Center for High Assurance Computing Systems (8/5/93). (Atkinson NRL, KX Records)	
	D35	Henning Schulzrinne, *Personal Mobility For Multimedia Services In The Internet*, Proceedings of the Interactive Distributed Multimedia Systems and Services European Workshop at 143 (1996). (Schulzrinne 96)	
	D36	Microsoft Corp., *Microsoft Virtual Private Networking: Using Point-to-Point Tunneling Protocol for Low-Cost, Secure, Remote Access Across the Internet* (1996) (printed from 1998 PDC DVD-ROM). (Point to Point, Microsoft Prior Art VPN Technology)	
	D37	"Safe Surfing: How to Build a Secure World Wide Web Connection," IBM Technical Support Organization, (March 1996). (Safe Surfing, WEBSITE ART)	
	D38	Goldschlag, et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK (May 1996). (Goldschlag II, Onion Routing)	
	D39	"IPSec Minutes From Montreal", IPSEC Working Group Meeting Notes, http://www.sandleman.ca/ipsec/1996/08/msg00018.html (June 1996). (IPSec Minutes, FreeS/WAN)	
	D40	J. M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California, July 1996. (Galvin, DNSSEC)	
	D41	J. Gilmore, et al. "Re: Key Management, anyone? (DNS Keying)," IPSec Working Group Mailing List Archives (8/96). (Gilmore DNS, FreeS/WAN)	
	D42	H. Orman, et al. "Re: 'Re: DNS? was Re: Key Management, anyone?" IETF IPSec Working Group Mailing List Archive (8/96-9/96). (Orman DNS, FreeS/WAN)	
	D43	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2052 (October 1996). (RFC 2052, DNS SRV)	
	D44	Freier, et al. "The SSL Protocol Version 3.0," Transport Layer Security Working Group (November 18, 1996). (SSL, UNDERLYING SECURITY TECHNOLOGY)	
	D45	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/02/1996). (RFC 2543 Internet Draft 1)	
	D46	M.G. Reed, et al. "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA, Dec. 9-13, 1996. (Reed, Onion Routing)	
	D47	Kenneth F. Alden & Edward P. Wobber, *The AltaVista Tunnel: Using the Internet to Extend Corporate Networks*, Digital Technical Journal (1997) (Alden, AltaVista)	
	D48	Automotive Industry Action Group, "ANX Release 1 Document Publication," AIAG (1997). (AIAG, ANX)	
	D49	Automotive Industry Action Group, "ANX Release 1 Draft Document Publication," AIAG Publications (1997). (AIAG Release, ANX)	
	D50	Aventail Corp. "Aventail VPN Data Sheet," *available at* http://www.archive.org/web/19970212013043/www.aventail.com/prod/vpndata.html (1997). (Data Sheet, Aventail)	
	D51	Aventail Corp., "Directed VPN Vs. Tunnel," *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/directvpn.html (1997). (Directed VPN, Aventail)	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

/Krisna Lim/ 01/26/2012

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

	D52	Aventail Corp., "Managing Corporate Access to the Internet," Aventail AutoSOCKS White Paper *available at* http://web.archive.org/199706200300312/www.aventail.com/educate/whitepaper/ipmw.html (1997). (Corporate Access, Aventail)	
	D53	Aventail Corp., "VPN Server V2.0 Administration Guide," (1997). (VPN, Aventail)	
	D54	Goldschlag, et al. "*Privacy on the Internet*," Naval Research Laboratory, Center for High Assurance Computer Systems (1997). (Goldschtag I, Onion Routing)	
	D55	Microsoft Corp., *Installing Configuring and Using PPTP with Microsoft Clients and Servers* (1997). (Using PPTP, Microsoft Prior Art VPN Technology)	
	D56	Microsoft Corp., *IP Security for Microsoft Windows NT Server 5.0* (1997) (printed from 1998 PDC DVD-ROM). (IP Security, Microsoft Prior Art VPN Technology)	
	D57	Microsoft Corp., *Microsoft Windows NT Active Directory: An Introduction to the Next Generation Directory Services* (1997) (printed from 1998 PDC DVD-ROM). (Directory, Microsoft Prior Art VPN Technology)	
	D58	Microsoft Corp., *Routing and Remote Access Service for Windows NT Server New Opportunities Today and Looking Ahead* (1997) (printed from 1998 PDC DVD-ROM). Routing, Microsoft Prior Art VPN Technology)	
	D59	Microsoft Corp., *Understanding Point-to-Point Tunneling Protocol PPTP* (1997) (printed from 1998 PDC DVD-ROM). (Understanding PPTP, Microsoft Prior Art VPN Technology)	
	D60	J. Mark Smith et.al., *Protecting a Private Network: The AltaVista Firewall*, Digital Technical Journal (1997). (Smith, AltaVista)	
	D61	Naganand Doraswamy *Implementation of Virtual Private Networks (VPNs) with IPSecurity*, <draft-ietf-ipsec-vpn-00.txt> (March 12, 1997). (Doraswamy)	
	D62	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (03/27/1997). (RFC 2543 Internet Draft 2)	
	D63	Aventail Corp., "Aventail and Cybersafe to Provide Secure Authentication For Internet and Intranet Communication," Press Release, April 3, 1997. (Secure Authentication, Aventail)	
	D64	D. Wagner, et al. "Analysis of the SSL 3.0 Protocol," (April 15, 1997). (Analysis, UNDERLYING SECURITY TECHNOLOGIES)	
	D65	Automotive Industry Action Group, "ANXO Certification Authority Service and Directory Service Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Definition, ANX)	
	D66	Automotive Industry Action Group, "ANXO Certification Process and ANX Registration Process Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Certification, ANX)	
	D67	Aventail Corp., "Aventail Announces the First VPN Solution to Assure Interoperability Across Emerging Security Protocols," June 2, 1997. (First VPN, Aventail)	
	D68	Syverson, et al. "Private Web Browsing," Naval Research Laboratory, Center for High 8 Assurance Computer Systems (June 2, 1997). (Syverson, Onion Routing)	
	D69	Bellcore, "Metrics, Criteria, and Measurement Technique Requirements for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (June 16, 1997). (AIAG Requirements, ANX)	
	D70	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/31/1997). (RFC 2543 Internet Draft 3)	
	D71	R. Atkinson, "Key Exchange Delegation Record for the DNS," Network Working Group, RFC 2230 (November 1997). (RFC 2230, KX Records)	
	D72	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/11/1997). (RFC 2543 Internet Draft 4)	
	D73	1998 Microsoft Professional Developers Conference DVD ("1998 PDC DVD-ROM") (including screenshots captured there from and produced as MSFTVX 00018827-00018832). (Conference, Microsoft Prior Art VPN Technology)	
	D74	Microsoft Corp., *Virtual Private Networking An Overview* (1998) (printed from 1998 PDC DVD-ROM) (Overview, Microsoft Prior Art VPN Technology)	
	D75	Microsoft Corp., *Windows NT 5.0 Beta Has Public Premiere at Seattle Mini-Camp Seminar attendees get first look at the performance and capabilities of Windows NT 5.0* (1998) (*available at* http://www.microsoft.com/presspass/features/1998/10-19nt5.mspxpftrue). (NT Beta, Microsoft Prior Art VPN Technology)	
	D76	"What ports does SSL use" *available at* stason.org/TULARC/security/ssl-talk/3-4-What-ports-does-ssl-use.html (1998). (Ports, DNS SRV)	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

/Krisna Lim/ 07/20/2012

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

	D77	Aventail Corp., "Aventail VPN V2.6 Includes Support for More Than Ten Authentication Methods Making Extranet VPN Development Secure and Simple," Press Release, January 19, 1998. (VPN V2.6, Aventail)	
	D78	R. G. Moskowitz, "Network Address Translation Issues with IPsec," Internet Draft, Internet Engineering Task Force, February 6, 1998. (Moskowitz)	
	D79	H. Schulzrinne, et al, "Internet Telephony Gateway Location," Proceedings of IEEE INfocom '98, The Conference on Computer Communications, Vol. 2 (March 29 – April 2, 1998). (Gateway, Schulzrinne)	
	D80	C. Huitema, 45 al. "Simple Gateway Control Protocol," Version 1.0 (May 5, 1998). (SGCP)	
	D81	DISA "Secret Internet Protocol Router Network," SIPRNET Program Management Office (D3113) DISN Networks, DISN Transmission Services (May 8, 1998). DISA, SIPRNET)	
	D82	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (05/14/1998). (RFC 2543 Internet Draft 5)	
	D83	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (06/17/1998). (RFC 2543 Internet Draft 6)	
	D84	D. McDonald, et al. "PF_KEY Key Management API, Version 2," Network Working Group, RFC 2367 (July 1998). (RFC 2367)	
	D85	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/16/1998). (RFC 2543 Internet Draft 7)	
	D86	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (08/07/1998). (RFC 2543 Internet Draft 8)	
	D87	Microsoft Corp., *Company Focuses on Quality and Customer Feedback* (August 18, 1998). (Focus, Microsoft Prior Art VPN Technology)	
	D88	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (09/18/1998). (RFC 2543 Internet Draft 9)	
	D89	Atkinson, et al. "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998). (RFC 2401, UNDERLYING SECURITY TECHNOLOGIES)	
	D90	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/12/1998). (RFC 2543 Internet Draft 10)	
	D91	Donald Eastlake, *Domain Name System Security Extensions*, IETF DNS Security Working Group (December 1998). (DNSSEC-7)	
	D92	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/15/1998). (RFC 2543 Internet Draft 11)	
	D93	Aventail Corp., "Aventail Connect 3.1/2.6 Administrator's Guide," (1999). (Aventail Administrator 3.1, Aventail)	
	D94	Aventail Corp., "Aventail Connect 3.1/2.6 User's Guide," (1999). (Aventail User 3.1, Aventail)	
	D95	Aventail Corp., "Aventail ExtraWeb Server v3.2 Administrator's Guide," (1999). (Aventail ExtraWeb 3.2, Aventail)	
	D96	Kaufman et al, "Implementing IPsec," (Copyright 1999). (Implementing IPSEC, VPN REFERENCES)	
	D97	Network Solutions, Inc. "Enabling SSL," NSI Registry (1999). (Enabling SSL, UNDERLYING SECURITY TECHNOLOGIES)	
	D98	Check Point Software Technologies Ltd. (1999) (Check Point, Checkpoint FW)	
	D99	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*,<draft-ietf-dnsind-frc2052bis-02.txt> (January 1999). (Gulbrandsen 99, DNS SRV)	
	D100	C. Scott, et al. *Virtual Private Networks*, O'Reilly and Associates, Inc., 2nd ed. (Jan. 1999). Scott VPNs)	
	D101	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (01/15/1999). (RFC 2543 Internet Draft 12)	
	D102	Goldschlag, et al., "Onion Routing for Anonymous and Private Internet Connections," Naval Research Laboratory, Center for High Assurance Computer Systems (January 28, 1999). (Goldschlag III, Onion Routing)	
	D103	H. Schulzrinne, "Internet Telephony: architecture and protocols – an IETF perspective," Computer Networks, Vol. 31, No. 3 (February 1999). (Telephony, Schulzrinne)	
	D104	M. Handley, et al. "SIP: Session Initiation Protocol," Network Working Group, RFC 2543 and Internet Drafts (12/96-3/99). (Handley, RFC 2543)	
	D105	FreeS/WAN Project, *Linux FreeS/WAN Compatibility Guide* (March 4, 1999). (FreeS/WAN Compatibility Guide, FreeS/WAN)	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

/Krisna Lim/ 07/20/2012

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

	D106	Telcordia Technologies, "ANX Release 1 Document Corrections," AIAG (May 11, 1999). (Telcordia, ANX)	
	D107	Ken Hornstein & Jeffrey Altman, *Distributing Kerberos KDC and Realm Information with DNS* <draft-eitf-cat-krb-dns-locate-oo.txt> (June 21, 1999). (Hornstein, DNS SRV)	
	D108	Bhattacharya, et al., "An LDAP Schema for Configuration and Administration of IPSec Based Virtual Private Networks (VPNs)", IETF Internet Draft (October 1999). (Bhattcharya LDAP VPN)	
	D109	B. Patel, et al. "DHCP Configuration of IPSEC Tunnel Mode," IPSEC Working Group, Internet Draft 02 (10/15/1999). (Patel)	
	D110	Goncalves, et al. *Check Point FireWall-1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW)	
	D111	"Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources," FirstVPN, (Jan 2000). (FirstVPN Microsoft)	
	D112	Gulbrandsen, Vixie, & Esibov, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2782 (February 2000). (RFC 2782, DNS SRV)	
	D113	MITRE Organization, "Technical Description," Collaborative Operations in Joint Expeditionary Force Experiment (JEFX) 99 (February 2000). (MITRE, SIPRNET)	
	D114	H. Schulzrinne, et al. "Application-Layer Mobility Using SIP," Mobile Computing and Communications Review, Vol. 4, No. 3. pp. 47-57 (July 2000). (Application, SIP)	
	D115	Kindred et al, "Dynamic VPN Communities: Implementation and Experience," DARPA Information Survivability Conference and Exposition II (June 2001). (DARPA, VPN SYSTEMS)	
	D116	ANX 101: Basic ANX Service Outline. (Outline, ANX)	
	D117	ANX 201: Advanced ANX Service. (Advanced, ANX)	
	D118	Appendix A: Certificate Profile for ANX IPsec Certificates. (Appendix, ANX)	
	D119	Assured Digital Products. (Assured Digital)	
	D120	Aventail Corp., "Aventail AutoSOCKS the Client Key to Network Security," Aventail Corporation White Paper. (Network Security, Aventail)	
	D121	Cindy Moran, "DISN Data Networks: Secret Internet Protocol Router Network (SIPRNet)." (Moran, SIPRNET)	
	D122	Data Fellows F-Secure VPN+ (F-Secure VPN+)	
	D123	"Interim Operational Systems Doctrine for the Remote Access Security Program (RASP) Secret Dial-In Solution. (RASP, SIPRNET)	
	D124	*Onion Routing*, "Investigation of Route Selection Algorithms," *available at* http://www.onion-router.net/Archives/Route/index.html. (Route Selection, Onion Routing)	
	D125	Secure Computing, "Bullet-Proofing an Army Net," Washington Technology. (Secure, SIPRNET)	
	D126	SPARTA "Dynamic Virtual Private Network." (Sparta, VPN SYSTEMS)	
	D127	Standard Operation Procedure for Using the 1910 Secure Modems. (Standard, SIPRNET)	
	D128	Publically available emails relating to FreeS/WAN (MSFTVX00018833-MSFTVX00019206). (FreeS/WAN emails, FreeS/WAN)	
	D129	Kaufman et al., "Implementing IPsec," (Copyright 1999) (Implementing IPsec)	
	D130	Network Associates *Gauntlet Firewall For Unix User's Guide Version 5.0* (1999). (Gauntlet User's Guide – Unix, Firewall Products)	
	D131	Network Associates *Gauntlet Firewall For Windows NT Getting Started Guide Version 5.0* (1999) (Gauntlet Getting Started Guide – NT, Firewall Products)	
	D132	Network Associates *Gauntlet Firewall For Unix Getting Started Guide Version 5.0* (1999) (Gauntlet Unix Getting Started Guide, Firewall Products)	
	D133	Network Associates *Release Notes Gauntlet Firewall for Unix 5.0* (March 19, 1999) (Gauntlet Unix Release Notes, Firewall Products)	
	D134	Network Associates *Gauntlet Firewall For Windows NT Administrator's Guide Version 5.0* (1999) (Gauntlet NT Administrator's Guide, Firewall Products)	
	D135	Trusted Information Systems, Inc. *Gauntlet Internet Firewall Firewall-to-Firewall Encryption Guide Version 3.1* (1996) (Gauntlet Firewall-to-Firewall, Firewall Products)	
	D136	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	D137	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	D138	Dan Sterne *Dynamic Virtual Private Networks* (May 23, 2000) (Sterne DVPN, DVPN)	
	D139	Darrell Kindred *Dynamic Virtual Private Networks (DVPN)* (December 21, 1999) (Kindred DVPN, DVPN)	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

/Krisna Lim/ 07/20/2012

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

	D140	Dan Sterne *et al. TIS Dynamic Security Perimeter Research Project Demonstration* (March 9, 1998) (Dynamic Security Perimeter, DVPN)	
	D141	Darrell Kindred *Dynamic Virtual Private Networks Capability Description* (January 5, 2000) (Kindred DVPN Capability, DVPN) 11	
	D142	October 7, and 28 1997 email from Domenic J. Turchi Jr. (SPARTA00001712-1714, 1808-1811) (Turchi DVPN email, DVPN)	
	D143	James Just & Dan Sterne *Security Quickstart Task Update* (February 5, 1997) (Security Quickstart, DVPN)	
	D144	Virtual Private Network Demonstration dated March 21, 1998 (SPARTA00001844-54) (DVPN Demonstration, DVPN)	
	D145	GTE Internetworking & BBN Technologies DARPA *Information Assurance Program Integrated Feasibilit Demonstration (IFD) 1.1 Plan* (March 10, 1998) (IFD 1.1, DVPN)	
	D146	Microsoft Corp. Windows NT Server Product Documentation: Administration Guide - Connection Point Services, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cpsops.mspx (Connection Point Services) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D147	Microsoft Corp. Windows NT Server Product Documentation: Administration Kit Guide - Connection Manager, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cmak.mspx (Connection Manager) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D148	Microsoft Corp. Autodial Heuristics, *available at* http://support.microsoft.com/kb/164249 (Autodial Heuristics) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D149	Microsoft Corp., Cariplo: Distributed Component Object Model, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms809332(printer).aspx (Cariplo I)	
	D150	Marc Levy, COM Internet Services (Apr. 23, 1999), *available at* http://msdn2.microsoft.com/en-us/library/ms809302(printer).aspx (Levy)	
	D151	Markus Horstmann and Mary Kirtland, DCOM Architecture (July 23, 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809311(printer).aspx (Horstmann)	
	D152	Microsoft Corp., DCOM: A Business Overview (Apr. 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809320(printer).aspx (DCOM Business Overview I)	
	D153	Microsoft Corp., DCOM Technical Overview (Nov. 1996), *available at* http://msdn2.microsoft.com/en-us/library/ms809340(printer).aspx (DCOM Technical Overview I)	
	D154	Microsoft Corp., DCOM Architecture White Paper (1998) *available in* PDC DVD-ROM (DCOM Architecture)	
	D155	Microsoft Corp, DCOM – The Distributed Component Object Model, A Business Overview White Paper (Microsoft 1997) *available in* PDC DVD-ROM (DCOM Business Overview II)	
	D156	Microsoft Corp., DCOM - Cariplo Home Banking Over The Internet White Paper Microsoft 1996) *available in* PDC DVD-ROM (Cariplo II)	
	D157	Microsoft Corp., DCOM Solutions in Action White Paper (Microsoft 1996) *available in* PDC DVD-ROM (DCOM Solutions in Action)	
	D158	Microsoft Corp., DCOM Technical Overview White Paper (Microsoft 1996) *available* 12 *in* PDC DVD-ROM (DCOM Technical Overview II)	
	D159	125. Scott Suhy & Glenn Wood, DNS and Microsoft Windows NT 4.0, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms810277(printer).aspx (Suhy)	
	D160	126. Aaron Skonnard, *Essential WinInet* 313-423 (Addison Wesley Longman 1998) (Essential WinInet)	
	D161	Microsoft Corp. Installing, Configuring, and Using PPTP with Microsoft Clients and Servers, (1998) *available at* http://msdn2.microsoft.com/enus/library/ms811078(printer).aspx (Using PPTP)	
	D162	Microsoft Corp., Internet Connection Services for MS RAS, Standard Edition, http://www.microsoft.com/techneUarchive/winntas/proddocs/inetconctservice/bcgstart.mspx (Internet Connection Services I)	

/Krisna Lim/ 07/20/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

	D163	Microsoft Corp., Internet Connection Services for RAS, Commercial Edition, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstrtc.mspx (Internet Connection Services II)	
	D164	Microsoft Corp., Internet Explorer 5 Corporate Deployment Guide – Appendix B: Enabling Connections with the Connection Manager Administration Kit, *available at* http://www.microsoft.com/technet/prodtechnol/ie/deploy/deploy5/appendb.mspx (IE5 Corporate Development)	
	D165	Mark Minasi, *Mastering Windows NT Server 4* 1359-1442 (6th ed., January 15, 1999) (Mastering Windows NT Server)	
	D166	*Hands On, Self-Paced Training for Supporting Version 4.0* 371-473 (Microsoft Press 1998) (Hands On)	
	D167	Microsoft Corp., MS Point-to-Point Tunneling Protocol (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/maintain/featusability/pptpwp3.mspx (MS PPTP)	
	D168	Kenneth Gregg, *et al., Microsoft Windows NT Server Administrator's Bible* 173-206, 883-911, 974-1076 (IDG Books Worldwide 1999) (Gregg)	
	D169	Microsoft Corp., Remote Access (Windows), *available at* http://msdn2.microsoft.com/enus/library/bb545687(VS.85.printer).aspx (Remote Access)	
	D170	Microsoft Corp., Understanding PPTP (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/plan/pptpudst.mspx (Understanding PPTP NT 4) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D171	Microsoft Corp., Windows NT 4.0: Virtual Private Networking, *available at* http://www.microsoft.com/technet/archive/winntas/deploy/confeat/vpntwk.mspx (NT4 VPN) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D172	Anthony Northrup, *NT Network Plumbing: Routers, Proxies, and Web Services* 299-399 (IDG Books Worldwide 1998) (Network Plumbing)	
	D173	Microsoft Corp., Chapter 1 - Introduction to Windows NT Routing with Routing and Remote Access Service, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/rras40/rrasch0l.mspx (Intro to RRAS) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.) 13	
	D174	Microsoft Corp., Windows NT Server Product Documentation: Chapter 5 - Planning for Large-Scale Configurations, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/rras40/rrasch05.mspx (Large-Scale Configurations) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	D175	F-Secure, *F-Secure NameSurfer*(May 1999) (from FSECURE 00000003) (NameSurfer 3)	
	D176	F-Secure, *F-Secure VPN Administrator's Guide* (May 1999) (from FSECURE 00000003) F-Secure VPN 3)	
	D177	F-Secure, *F-Secure SSH User's & Administrator's Guide* (May 1999) (from FSECURE 00000003) (SSH Guide 3)	
	D178	F-Secure, *F-Secure SSH2.0 for Windows NT and 95* (May 1999) (from FSECURE 00000003) (SSH 2.0 Guide 3)	
	D179	F-Secure, *F-Secure VPN+ Administrator's Guide* (May 1999) (from FSECURE 00000003) (VPN+ Guide 3)	
	D180	F-Secure, *F-Secure VPN+ 4.1* (1999) (from FSECURE 00000006) (VPN+ 4.1 Guide 6)	
	D181	F-Secure, *F-Secure SSH* (1996) (from FSECURE 00000006) (F-Secure SSH 6)	
	D182	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (1998) (from FSECURE 00000006) (F-Secure SSH 2.0 Guide 6)	
	D183	F-Secure, *F-Secure SSH User's & Administrator's Guide* (Sept. 1998) (from FSECURE 00000009) (SSH Guide 9)	
	D184	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (Sept. 1998) (from FSECURE 00000009) (F-Secure SSH 2.0 Guide 9)	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

/Krisna Lim/ 07/20/2012

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

	D185	F-Secure, *F-Secure VPN+* (Sept. 1998) (from FSECURE 00000009) (VPN+ Guide 9)	
	D186	F-Secure, *F-Secure Management Tools, Administrator's Guide* (1999) (from FSECURE 00000003) (F-Secure Management Tools)	
	D187	F-Secure, *F-Secure Desktop, User's Guide* (1997) (from FSECURE 00000009) (FSecure Desktop User's Guide)	
	D188	SafeNet, Inc., *VPN Policy Manager* (January 2000) (VPN Policy Manager)	
	D189	F-Secure, *F-Secure VPN+ for Windows NT 4.0* (1998) (from FSECURE 00000009) (FSecure VPN+)	
	D190	IRE, Inc., *SafeNet/Security Center Technical Reference Addendum* (June 22, 1999) (Safenet Addendum)	
	D191	IRE, Inc., *System Description for VPN Policy Manager and SafeNet/SoftPK* (March 30, 2000) (VPN Policy Manager System Description)	
	D192	IRE, Inc., *About SafeNet / VPN Policy Manager* (1999) (About Safenet VPN Policy Manager)	
	D193	Trusted Information Systems, Inc., *Gauntlet Internet Firewall, Firewall Product Functional Summary* July 22, 1996) (Gauntlet Functional Summary)	
	D194	Trusted Information Systems, Inc., *Running the Gauntlet Internet Firewall, An Administrator's Guide to Gauntlet Version 3.0* (May 31, 1995) (Running the Gauntlet Internet Firewall)	
	D195	Ted Harwood, *Windows NT Terminal Server and Citrix Metaframe* (New Riders 1999) (Windows NT Harwood) 79	
	D196	Todd W. Mathers and Shawn P. Genoway, *Windows NT Thing Client Solutions: Implementing Terminal Server and Citrix MetaFrame* (Macmillan Technical Publishing 1999) (Windows NT Mathers)	
	D197	Bernard Aboba et al., *Securing L2TP using IPSEC* (February 2, 1999)	
	D198	156. *Finding Your Way Through the VPN Maze* (1999) ("PGP")	
	D199	Linux FreeS/WAN Overview (1999) (Linux FreeS/WAN Overview)	
	D200	TimeStep, *The Business Case for Secure VPNs* (1998) ("TimeStep")	
	D201	WatchGuard Technologies, Inc., *WatchGuard LiveSecurity for MSS Powerpoint* (Feb. 14 2000)	
	D202	WatchGuard Technologies, Inc., *MSS Version 2.5, Add-On for WatchGuard SOHO Releaset Notes* (July 21, 2000)	
	D203	WatchGuard Technologies, Inc., *MSS Firewall Specifications* (1999)	
	D204	WatchGuard Technologies, Inc., *Request for Information, Security Services* (2000)	
	D205	WatchGuard Technologies, Inc., *Protecting the Internet Distributed Enterprise, White Paper* (February 2000)	
	D206	Air Force Research Laboratory, *Statement of Work for Information Assurance System Architecture and Integration, PR No. N-8-6106 (Contract No. F30602-98-C-0012)* (January 29, 1998)	
	D207	Technologies, Inc., *WatchGuard Firebox System Powerpoint* (2000)	
	D208	GTE Internetworking & BBN Technologies DARPA *Information Assurance Program Integrated Feasibility Demonstration 1FD 1.2 Report, Rev. 1.0* (September 21, 1998)	
	D209	BBN Information Assurance Contract, *TIS Labs Monthly Status Report* (March 16-April 30, 1998)	
	D210	DARPA, *Dynamic Virtual Private Network (VPN) Powerpoint*	
	D211	GTE Internetworking, *Contractor's Program Progress Report* (March 16-April 30, 1998)	
	D212	Darrell Kindred, *Dynamic Virtual Private Networks (DVPN) Countermeasure Characterization* (January 30, 2001)	
	D213	*Virtual Private Networking Countermeasure Characterization* (March 30, 2000)	
	D214	*Virtual Private Network Demonstration* (March 21, 1998)	
	D215	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks (VPNs) and Integrated Security Management* (2000)	
	D216	Information Assurance/NAI Labs, *Create/Add DVPN Enclave* (2000)	
	D217	NAI Labs, *IFE 3.1 Integration Demo* (2000)	
	D218	Information Assurance, *Science Fair Agenda* (2000)	
	D219	Darrell Kindred et al., *Proposed Threads for IFE 3.1* (January 13, 2000)	
	D220	*IFE 3.1 Technology Dependencies* (2000)	
	D221	*IFE 3.1 Topology* (February 9, 2000)	
	D222	Information Assurance, *Information Assurance Integration: IFE 3.1, Hypothesis & Thread Development* January 10-11, 2000)	
	D223	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation* (2000)	
	D224	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.2* (2000)	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

/Krisna Lim/ 07/20/2012

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

	D225	Information Assurance/NAI Labs, Dynamic Virtual Private Networks Presentation v.3 (2000)	
	D226	T. Braun et al., *Virtual Private Network Architecture*, Charging and Accounting Technology for the Internet (August 1, 1999) (VPNA)	
	D227	Network Associates Products - *PGP Total Network Security Suite, Dynamic Virtual Private Networks* (1999)	
	D228	Microsoft Corporation, *Microsoft Proxy Server 2.0* (1997) (Proxy Server 2.0, Microsoft Prior Art VPN Technology)	
	D229	David Johnson et. al., *A Guide To Microsoft Proxy Server 2.0* (1999) (Johnson, Microsoft Prior Art VPN Technology)	
	D230	Microsoft Corporation, *Setting Server Parameters* (1997 (copied from Proxy Server 2.0 CD labeled MSFTVX00157288) (Setting Server Parameters, Microsoft Prior Art VPN Technology)	
	D231	Kevin Schuler, *Microsoft Proxy Server 2* (1998) (Schuler, Microsoft Prior Art VPN Technology)	
	D232	Erik Rozell et. al., *MCSE Proxy Server 2 Study Guide* (1998) (Rozell, Microsoft Prior 15 Art VPN Technology)	
	D233	M. Shane Stigler & Mark A Linsenbardt, *IIS 4 and Proxy Server 2* (1999) (Stigler, Microsoft Prior Art VPN Technology)	
	D234	David G. Schaer, *MCSE Test Success: Proxy Server 2*(1998) (Schaer, Microsoft Prior Art VPN Technology)	
	D235	John Savill, *The Windows NT and Windows 2000 Answer Book* (1999) (Savill, Microsoft Prior Art VPN Technology)	
	D236	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	D237	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	D238	File History for U.S. Application Serial No. 09/653,201, Applicant(s): Whittle Bryan, et al., Filing Date 08/31/2000.	
	D239	*AutoSOCKS v2. 1*, Datasheet, http://web.archive.org/web/19970212013409/www.aventail.com/prod/autoskds.html	
	D240	Ran Atkinson, *Use of DNS to Distribute Keys*, 7 Sept. 1993, http://ops.ietf.org/lists/namedroppers/namedroppers, 1 99x/msg00945.html	
	D241	FirstVPN Enterprise Networks, Overview	
	D242	Chapter 1: Introduction to Firewall Technology, Administration Guide; 12/19/07, http://www.books24x7.com/book/id_762/viewer_r.asp?bookid=762&chunked=41065062	
	D243	The TLS Protocol Version 1.0; January 1999; page 65 of 71.	
	D244	Elizabeth D. Zwicky, et al., Building Internet Firewalls, 2nd Ed.	
	D245	Virtual Private Networks - Assured Digital Incorporated - ADI 4500; http://web.archive.org/web/19990224050035/www.assured-digital.com/products/prodvpn/adia4500.htm	
	D246	Accessware - The Third Wave in Network Security, Conclave from Internet Dynamics; http://web.archive.org/web/11980210013830/interdyn.com/Accessware.html	
	D247	Extended System Press Release, Sept. 2, 1997; *Extended VPN Uses The Internet to Create Virtual Private Networks*, www.extendedsystems.com	
	D248	Socks Version 5; Executive Summary; http://web.archive.org/web/199970620031945/www.aventail.com/educate/whitepaper/sockswp.html	
	D249	Internet Dynamics First to Ship Integrated Security Solutions for Enterprise Intranets and Extranets; Sept. 15, 1997; http://web.archive.org/web/19980210014150/interdyn.com	
	D250	Emails from various individuals to Linux IPsec re: DNS-LDAP Splicing	
	D251	Fasbender, A., et al., Variable and Scalable Security: Protection of Location Information in Mobile IP, IEEE VTS, 46th, 1996, 5 pp.	
	D252	David Kosiur, "Building and Managing Virtual Private Networks" (1998)	
	D253	Request for Inter Partes Reexamination of Patent No. 6,502,135, dated Nov. 25, 2009.	
	D254	Request for Inter Partes Reexamination of Patent No. 7,188,180, dated Nov. 25, 2009.	
	D255	Yuan Dong Feng, "A novel scheme combining interleaving technique with cipher in Rayleigh fading channels," Proceedings of the International Conference on Communication technology, 2:S47-02-1-S47-02-4 (1998)	

/Krisna Lim/ 07/20/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

	D256	Davies and Price, edited by Tadahiro Uezono, "Network Security", Japan, Nikkei McGraw-Hill, December 5, 1958, First Edition, first copy, p. 102-108	
	D257	Davies et al., "An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer," Security for Computer Networks, Second Edition, pp. 98-101 (1989)	
	D258	Baumgartner et al, "Differentiated Services: A New Approach for Quality of Service in the Internet," International Conference on High Performance Networking, 255-273 (1998)	
	D259	Chapman et al., "Domain Name System (DNS)," 278-296 (1995)	
	D260	Davila et al., "Implementation of Virtual Private Networks at the Transport Layer," M. Mambo, Y. Zheng (Eds), Information Security (Second International) Workshop, ISW' 99. Lecture Notes in Computer Science (LNCS), Vol. 1729; 85-102 (1999)	
	D261	De Raadt et al., "Cryptography in OpenBSD," 10 pages (1999)	
	D262	Eastlake, "Domain Name System Security Extensions," Internet Citation, Retrieved from the Internet: URL:ftp://ftp.inet.no/pub/ietf/internet-drafts/draft-ietf-dnssec-secext2-05.txt (1998)	
	D263	Gunter et al., "An Architecture for Managing QoS-Enabled VRNs Over the Internet," Proceedings 24th Conference on Local Computer Networks. LCN' 99 IEEE Comput. Soc Los Alamitos, CA, pages 122-131 (1999)	
	D264	Shimizu, "Special Feature: Mastering the Internet with Windows 2000", Internet Magazine, 63:296-307 (2000)	
	D265	Stallings, "Cryptography and Network Security," Principals and Practice, 2nd Edition, pages 399-440 (1999)	
	D266	Takata, "U.S. Vendors Take Serious Action to Act Against Crackers – A Tracking Tool and a Highly Safe DNS Software are Released", Nikkei Communications, 257:87(1997)	
	D267	Wells, Email (Lancasterb1be@mail.msn.com), Subject: "Security Icon," (1998)	
	D268	Microsoft Corporation's Fifth Amended Invalidity Contentions dated September 18, 2009, VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation and invalidity claim charts for U.S. Patent Nos. 7,188,180 and 6,839,759	
	D269	The IPSEC Protocol as described in Atkinson, et al., "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998) ("RFC 2401"); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D270	S. Kent and R. Atkinson, "IP Authentication Header," RFC 2402 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D271	C. Madson and R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH," RFC 2403 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D272	C. Madson and R. Glenn, "The Use HMAC-SHA-1-96 within ESP and AH," RFC 2404 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D273	C. Madson and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV", RFC 2405 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	

/Krisna Lim/ 07/20/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

	D274	S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," RFC 2406 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D275	Derrell Piper, "The Internet IP Security Domain of Interpretation for ISAKMP," RFC 2407 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D276	Douglas Maughan, et al, "Internet Security Association and Key Management Protocol (ISAKMP)," RFC 2408 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D277	D. Harkins and D. Carrell, "The Internet Key Exchange (IKE)," RFC 2409 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D278	R. Glenn and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec." RFC 2410 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D279	R. Thayer, et al., "IP Security Document Roadmap," RFC 2411 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	D280	Hilarie K. Orman, "The OAKLEY Key Determination Protocol," RFC 2412 (November 1998) in combination with J.M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose California (July 1996) ("Galvin")	
	D281	DNS-related correspondence dated September 7, 1993 to September 20, 1993. (Pre KX, KX Records)	
	D282	Aventail Corp., "AutoSOCKS v. 2.1 Datasheet," *available at* http://www.archive.org/web/19970212013409/www.aventail.com/prod/autosk2ds.html (1997). (AutoSOCKS, Aventail)	
	D283	Aventail Corp., "Socks Version 5," Aventail Whitepaper, *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/soc kswp.html (1997). (Socks, Aventail)	
	D284	Goncalves, et al. *Check Point FireWall -1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW)	
	D285	Assured Digital Products. (Assured Digital)	
	D286	F-Secure, *F-Secure Evaluation Kit* (May 1999) (FSECURE 00000003) (Evaluation Kit 3)	
	D287	F-Secure, *F-Secure Evaluation Kit* (Sept. 1998) (FSECURE 00000009) (Evaluation Kit 9)	
	D288	IRE, Inc., *SafeNet/Soft-PK Version 4* (March 28, 2000) (Soft-PK Version 4)	
	D289	IRE/SafeNet Inc., *VPN Technologies Overview* (March 28, 2000) (Safenet VPN Overview)	
	D290	IRE, Inc., *SafeNet/VPN Policy Manager Quick Start Guide Version 1* (1999) (SafeNet VPN Policy Manager)	
	D291	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.3* (2000)	
	D292	PCT International Search Report for related PCT Application No.: PCT/US01/13261, 8 pages .	
	D293	PCT International Search Report for related PCT Application No.: PCT/US99/25323, 3 pages .	
	D294	PCT International Search Report for related PCT Application No.: PCT/US99/25325, 3 pages .	
	D295	Deposition Transcript for Gary Tomlinson dated February 27, 2009	
	D296	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 8, 2010, 8:45 AM	
	D297	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 8, 2010, 1:30 PM	
	D298	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 9, 2010, 9:00 AM	

/Krisna Lim/ 07/20/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

	D299	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 9, 2010, 1:30 PM	
	D300	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 10, 2010, 9:00 AM	
	D301	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 10, 2010, 1:00 PM	
	D302	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 11, 2010, 9:00 AM	
	D303	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 11, 2010, 1:30 PM	
	D304	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 12, 2010, 9:00 AM	
	D305	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 12, 2010, 1:15 PM	
	D306	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 15, 2010, 9:00 AM	
	D307	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 15, 2010, 12:35 PM	
	D308	European Search Report dated January 24, 2011 from corresponding European Application Number 10011949.4	
	D309	European Search Report dated March 17, 2011 from corresponding European Application Number 10184502.2	
	D310	Hollenbeck et al., "Registry Registrar Protocol (RRP) Version 1.1.0; Internet Engineering Task Force, 34 pages (1999)	
	D311	Tannenbaum, "Computer Networks," pages 202-219 (1996)	
	D312	Defendants' Preliminary Joint Invalidity Contentions dated July 1, 2011	
	D313	Appendix B: DNS References to Defendants' Preliminary Joint Invalidity Contentions dated July 1, 2011	
	D314	Appendix A to Defendants' Preliminary Joint Invalidity Contentions dated July 1, 2011	
	D315	Exhibit 1, IETF RFC 2065: Domain Name System Security Extensions; Published January 1997[1] vs. Claims of the '211 Patent[2]	
	D316	Exhibit 2, IETF RFC 2065: Domain Name System Security Extensions; Published January 1997[1] vs. Claims of the '504 Patent[2]	
	D317	Exhibit 3, RFC 2543[1] vs. Claims of the '135 Patent[2]	
	D318	Exhibit 4, RFC 2543[1] vs. Claims of the '211 Patent[2]	
	D319	Exhibit 5, RFC 2543[1] vs. Claims of the '504 Patent[2]	
	D320	Exhibit 6, SIP Draft v.2[1] vs. Claims of the '135 Patent[2]	
	D321	Exhibit 7, SIP Draft v.2[1] vs. Claims of the '211 Patent[2]	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

/Krisna Lim/ 07/20/2012

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	13/336,790
Filing Date	12-23-2011
First Named Inventor	Victor Larson
Art Unit	2165
Examiner Name	Krisna Lim
Docket Number	77580-151(VRNK-0001CP3CNFT1)

	D322	Exhibit 8, SIP Draft v.2[1] vs. Claims of the '504 Patent[2]	
	D323	Exhibit 9, H.323[1] vs. Claims of the '135 Patent[2]	
	D324	Exhibit 10, H.323[1] vs. Claims of the '211 Patent[2]	
	D325	Exhibit 11, H.323[1] vs. Claims of the '504 Patent[2]	
	D326	Exhibit 12, SSL 3.0[1] vs. Claims of the '135 Patent[2].	
	D327	Exhibit 13, SSL 3.0[1] vs. Claims of the '211 Patent[2]	
	D328	Exhibit 14, SSL 3.0[1] vs. Claims of the '504 Patent[2]	
	D329	Exhibit 15, RFC 2487[1] vs. Claims of the '135 Patent[2]	
	D330	Exhibit 16, RFC 2487[1] vs. Claims of the '211 Patent[2]	
	D331	Exhibit 17, RFC 2487[1] vs. Claims of the '504 Patent[2]	
	D332	Exhibit 18, RFC 2595[1] vs. Claims of the '135 Patent[2]	
	D333	Exhibit 19, RFC 2595[1] vs. Claims of the '211 Patent[2]	
	D334	Exhibit 20, RFC 2595[1] vs. Claims of the '504 Patent[2]	
	D335	Exhibit 21, iPass[1] vs. Claims of the '135 Patent[2]	
	D336	Exhibit 22, iPASS[1] vs. Claims of the '211 Patent[2]	
	D337	Exhibit 23, iPASS[1] vs. Claims of the '504 Patent[2]	
	D338	Exhibit 24, "US '034"[1] vs. Claims of the '135 Patent[2]	
	D339	Exhibit 25, US Patent No. 6,453,034 ("US '034")[1] vs. Claims of the '211 Patent[2]	
	D340	Exhibit 26, US Patent No. 6,453,034 ("US '034")[1] vs. Claims of the '504 Patent[2]	
	D341	Exhibit 27, US '287[1] vs. Claims of the '135 Patent[2]	
	D342	Exhibit 28, US '287[1] vs. Claims of the '211 Patent[2]	
	D343	Exhibit 29, US '287[1] vs. Claims of the '504 Patent[2]	
	D344	Exhibit 30, Overview of Access VPNs[1] vs. Claims of the '135 Patent[2]	
	D345	Exhibit 31, Overview of Access VPNs[1] vs. Claims of the '211 Patent[2]	
	D346	Exhibit 32, Overview of Access VPNs[1] vs. Claims of the '504 Patent[2]	
	D347	Exhibit 34, RFC 1928[1] vs. Claims of the '135 Patent[2]	

/Krisna Lim/ 07/20/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./