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:

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 [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

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:

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, Victor
Family Name / First Given Name / Second Given Name
Residence Fairfax, Virginia Citizenship USA
Post Office Address 12026 Lisa Marie Court, Fairfax, Virginia 22033

Signature Robert D. Short III Date 11/7/03
Full Name of Second Inventor Short, III, Robert, Dunham
Family Name / First Given Name / 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, Edmund, Colby
Family Name / First Given Name / 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, Michael
Family Name / First Given Name / Second Given Name
Residence South Riding, Virginia Citizenship USA
Post Office Address 26203 Ocala Circle, South Riding, Virginia 20152

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:

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

Attorney Docket No.: 077580-0177

U.S. PATENT APPLICATION FOR

AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

Inventors: Victor LARSON, a citizen of the United States, residing at 12026 Lisa Marie Court, Fairfax, Virginia 22033

Robert Dunham SHORT, III, a citizen of the United States, residing at 38710 Goose Creek Lane, Leesburg, Virginia 20175

Edmund Colby MUNGER, a citizen of the United States, residing at 1101 Opaca Court, Crownsville, Maryland 21032

Michael WILLIAMSON, a citizen of the United States, residing at 26203 Ocala Circle, South Riding, Virginia 20152

Assignee: VIRNETX, INC.
P.O. Box 439
Zephyr Cove, Nevada 89448

Entity: Large

McDERMOTT WILL & EMERY LLP
28 State Street
Boston, MA 02109-1775
617.535.4000

DM_US 38877810-1.077580.0177

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, 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 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, all of which are hereby incorporated by reference in their entirety for all purposes. The subject matter of U.S. application serial number 09/429,643 derives from provisional U.S. Application Nos. 60/106,261 (filed October 30, 1998) and 60/137,704 (filed June 7, 1999), all of which are hereby incorporated by reference in their entirety for all purposes. The present application is also related to U.S. application serial number 09/558,209, filed April 26, 2000, now abandoned, which is hereby incorporated by reference in its entirety for all purposes.

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.

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 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 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 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 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.

[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.

BRIEF DESCRIPTION OF THE DRAWINGS

[0031] FIG. 1 is an illustration of secure communications over the Internet according to a prior art embodiment.

[0032] FIG. 2 is an illustration of secure communications over the Internet according to an embodiment of the invention.

[0033] FIG. 3A is an illustration of a process of forming a tunneled IP packet according to an embodiment of the invention.

[0034] FIG. 3B is an illustration of a process of forming a tunneled IP packet according to another embodiment of the invention.

[0035] FIG. 4 is an illustration of an OSI layer location of processes that may be used to implement the invention.

[0036] FIG. 5 is a flow chart illustrating a process for routing a tunneled packet according to an embodiment of the invention.

[0037] FIG. 6 is a flow chart illustrating a process for forming a tunneled packet according to an embodiment of the invention.

[0038] FIG. 7 is a flow chart illustrating a process for receiving a tunneled packet according to an embodiment of the invention.

[0039] FIG. 8 shows how a secure session is established and synchronized between a client and a TARP router.

[0040] FIG. 9 shows an IP address hopping scheme between a client computer and TARP router using transmit and receive tables in each computer.

[0041] FIG. 10 shows physical link redundancy among three Internet Service Providers (ISPs) and a client computer.

[0042] 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.

[0043] FIG. 12A shows a system that employs hopped hardware addresses, hopped IP addresses, and hopped discriminator fields.

[0044] FIG. 12B shows several different approaches for hopping hardware addresses, IP addresses, and discriminator fields in combination.

[0045] FIG. 13 shows a technique for automatically re-establishing synchronization between sender and receiver through the use of a partially public sync value.

[0046] FIG. 14 shows a "checkpoint" scheme for regaining synchronization between a sender and recipient.

[0047] FIG. 15 shows further details of the checkpoint scheme of FIG. 14.

[0048] FIG. 16 shows how two addresses can be decomposed into a plurality of segments for comparison with presence vectors.

[0049] FIG. 17 shows a storage array for a receiver's active addresses.

[0050] FIG. 18 shows the receiver's storage array after receiving a sync request.

[0051] FIG. 19 shows the receiver's storage array after new addresses have been generated.

[0052] FIG. 20 shows a system employing distributed transmission paths.

[0053] FIG. 21 shows a plurality of link transmission tables that can be used to route packets in the system of FIG. 20.

[0054] FIG. 22A shows a flowchart for adjusting weight value distributions associated with a plurality of transmission links.

[0055] FIG. 22B shows a flowchart for setting a weight value to zero if a transmitter turns off.

[0056] FIG. 23 shows a system employing distributed transmission paths with adjusted weight value distributions for each path.

[0057] FIG. 24 shows an example using the system of FIG. 23.

[0058] FIG. 25 shows a conventional domain-name look-up service.

[0059] FIG. 26 shows a system employing a DNS proxy server with transparent VPN creation.

[0060] FIG. 27 shows steps that can be carried out to implement transparent VPN creation based on a DNS look-up function.

[0061] FIG. 28 shows a system including a link guard function that prevents packet overloading on a low-bandwidth link LOW BW.

[0062] FIG. 29 shows one embodiment of a system employing the principles of FIG. 28.

[0063] FIG. 30 shows a system that regulates packet transmission rates by throttling the rate at which synchronizations are performed.

[0064] FIG. 31 shows a signaling server 3101 and a transport server 3102 used to establish a VPN with a client computer.

[0065] FIG. 32 shows message flows relating to synchronization protocols of FIG. 31.

[0066] 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.

[0067] 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.

[0068] FIG. 35 shows a flow diagram for registering a secure domain name according to the present invention.

[0069] 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.

[0070] 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

[0071] 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.

[0072] 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.

[0073] 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.

[0074] 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.

[0075] 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.

[0076] 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.

[0077] 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.

[0078] 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*.

[0079] 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.

[0080] 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.

[0081] 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.

[0082] 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.

[0083] 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.

[0084] 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.

[0085] 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.

[0086] 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.

[0087] 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.

[0088] 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.

[0089] 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.

[0090] 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.

[0091] 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.

[0092] 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.

- 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.

[0093] 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.

[0094] 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

[0095] 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.

[0096] 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.

[0097] 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.

[0098] 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.

[0099] 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.

[00100] 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.

[00101] 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.

[00102] 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.

[00103] 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.

[00104] 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.

[00105] 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.

[00106] 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.

[00107] 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.

[00108] 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.

[00109] 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

[00110] 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.

[00111] 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

[00112] 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.

[00113] 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.

[00114] 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.

[00115] 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.

[00116] 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.

[00117] 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.

[00118] 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.

[00119] 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.

[00120] 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.

[00121] 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.

[00122] 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.

[00123] 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.

[00124] 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.

[00125] 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.

[00126] 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).

[00127] 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.

[00128] 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.)

[00129] 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

[00130] 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.

[00131] 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

[00132] 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.

[00133] 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.

[00134] 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.

[00135] 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.

[00136] 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.

[00137] 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.

[00138] 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.

[00139] 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.

[00140] 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.

[00141] 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.

[00142] 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.

[00143] 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.

[00144] 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

[00145] 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.

[00146] 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.

[00147] 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.

[00148] 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.

[00149] 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).

[00150] 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.

[00151] 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

[00152] 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.

[00153] 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:

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

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

[00154] $(X_0(a-1)+b)$ 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).

[00155] 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 j^{th} checkpoint, as X_0 and *n* as *i*, a node can store $a^n \bmod((a-1)c)$ once per LCR and set

[00156] $X_{j+1}{}^w=X_{n(j+1)}=((a^n \bmod((a-1)c)\ (X_j{}^w\ (a-1)+b)-b)/(a-1)) \bmod c$, (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).

[00157] 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.

[00158] 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

[00159] 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:

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

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

TABLE 1

I	X_i	$(X_i 30+4)$	$91\ (X_i 30+4)-4$	$((91\ (X_i 30+4)-4)/30$	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

[00160] 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.

[00161] 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:

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

5. 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).

6. 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.

[00162] 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

[00163] 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 x^{th} 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."

[00164] For example, suppose one wanted to represent the number 135 using a presence vector. The 135^{th} 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 135^{th} 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.

[00165] 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).

[00166] A presence vector will have a 1 in the y^{th} 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.

[00167] 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.

[00168] 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

[00169] 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 ≤OoO ≤WINDOW_SIZE and WINDOW_SIZE ≥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.

[00170] 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.

[00171] 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:

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

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

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

10. 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

[00172] 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.

[00173] 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

[00174] 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

[00175] 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.

[00176] 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).

[00177] 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.

[00178] 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.

[00179] 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.

[00180] 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.

[00181] 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.

[00182] 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.

[00183] 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.

[00184] 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.

[00185] 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).

[00186] 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.

[00187] 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.

[00188] 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).

[00189] 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.

[00190] 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.

[00191] 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.

[00192] 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.

[00193] 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.

[00194] 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.

[00195] 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.

[00196] 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:

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

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:

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

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

[00197] Equation 2 will increase the traffic weight to S during sustained periods of acceptable service in a damped exponential fashion.

[00198] 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).

[00199] 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 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

[00200] A second improvement concerns the automatic creation of a virtual private network (VPN) in response to a domain-name server look-up function.

[00201] 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.

[00202] 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.

[00203] 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.

[00204] 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).

[00205] 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.

[00206] 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.

[00207] 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.

[00208] 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.

[00209] 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.

[00210] 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.

[00211] 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.

[00212] 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.

[00213] 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.

[00214] 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.

[00215] 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:

[00216] 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.

[00217] 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.

[00218] 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.

[00219] 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

[00220] 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.

[00221] 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.

[00222] 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.

[00223] 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).

[00224] 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].

[00225] 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).

[00226] 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.

[00227] 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.

[00228] 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.

[00229] 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

[00230] 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.

[00231] 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.

[00232] 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.

[00233] 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.

[00234] Two practical issues should be considered when implementing the above scheme:

7. 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.

8. 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.

[00235] 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.

[00236] 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.

[00237] 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).

[00238] 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.

[00239] 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

[00240] 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.

[00241] 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.

[00242] 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.

[00243] 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.

[00244] 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.

[00245] 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.

[00246] 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.

[00247] 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.

[00248] 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.

[00249] 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.

[00250] 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.

[00251] Assuming that a client application wishes to send a packet to the server on the client's standing signaling VPL:

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.

[00252] 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.

[00253] 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.

[00254] 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.

[00255] 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

[00256] 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.

[00257] 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.

[00258] 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.

[00259] 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."

[00260] 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 computer network 3302. At step 3406, the communication link between computer 3301 and website 3308 is then terminated in a well-known manner.

[00261] 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.

[00262] 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.

[00263] 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.

[00264] 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.

[00265] 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.

[00266] 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.

[00267] 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.

[00268] 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 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.

[00269] 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.

[00270] 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.

[00271] 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".

[00272] 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.

[00273] 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.

[00274] 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

[00275] 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.

[00276] 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.

[00277] 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.

[00278] 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.

[00279] 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.

[00280] 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.

[00281] 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 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.

[00282] 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.

[00283] 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.

[00284] 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.

[00285] 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.

[00286] 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.

[00287] 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.

[00288] 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 method of transparently creating an encrypted communications channel between a client device and a target device, each device being configured to allow audio video communications between the client device and the target device over the encrypted communications channel once the encrypted communications channel is created, the method comprising:

(1) receiving from the client device a request for a network address associated with the target device;

(2) determining whether the request transmitted in step (1) is requesting access to a device that accepts an encrypted channel connection with the client device; and

(3) in response to determining that the address request in step (2) is requesting access to a device that accepts an encrypted communications channel connection with the client device, providing provisioning information required to initiate the creation of the encrypted communications channel between the client device and the target device such that the encrypted communications channel supports secure audio/video communications transmitted between the two devices.

2. The method of claim 1, wherein providing the provisioning information required to initiate the encrypted communications channel is based on a determination that the target device is a device with which an encrypted communications channel can be established when the address request corresponds to a target device identified in an network address lookup.

3. The method of claim 1, wherein the encrypted communications channel is a virtual private network link.

4. The method of claim 1, wherein the address request includes a secure domain name.

5. The method of claim 1, wherein the encrypted communications channel is a broadband connection.

6. The method of claim 1, wherein the encrypted communications channel is a unmodulated transmission link.

7. The method of claim 1, wherein the encrypted communications channel is a umodulated transmission link.

8. The method of claim 1, wherein the encrypted communications channel supports at least one of the following: FTM, TDM and CDMA.

9. The method of claim 1, wherein the client device is a phone.

10. The method of claim 9, wherein providing the provisioning information required to initiate the encrypted communications channel is based on a determination that the target device is a device with which an encrypted communications channel can be established when the address request corresponds to a target device identified in an network address lookup

11. The method of claim 9, wherein the encrypted communications channel is a virtual private network link.

12. The method of claim 9, wherein the address request includes a secure domain name.

13. The method of claim 9, wherein the encrypted communications channel is a broadband connection.

14. The method of claim 9, wherein the encrypted communications channel is a unmodulated transmission link.

15. The method of claim 9, wherein the encrypted communications channel is a modulated transmission link.

16. The method of claim 9, wherein the encrypted communications channel supports at least one of the following: FTM, TDM and CDMA.

17. The method of claim 9, wherein the target device is a server.

18. The method of claim 9, wherein the target device is a phone.

19. A system for transparently creating an encrypted communications channel between a client device and a target device, each device being configured to allow audio video communications therebetween over an encrypted communications channel once the encrypted communications channel is created, the system including a server configuration arranged to:

(1) receive from the client device a request for a network address associated with the target device;

(2) determine whether the request transmitted in step (1) is requesting access to a device that accepts an encrypted channel connection with the client device; and

(3) in response to determining that the address request in step (2) is requesting access to a device that accepts an encrypted communications channel connection with the client device, provide provisioning information required to initiate the creation of the encrypted communications channel between the client device and the target device such that the encrypted communications channel supports secure audio/video communications transmitted between the two devices.

20. A system according to claim 19, wherein the encrypted communications channel supports a plurality of services comprising a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof.

ABSTRACT

A method is used to transparently create an encrypted communications channel between a client device and a target device. Each device is configured to allow audio video communications between the client device and the target device over the encrypted communications channel once the encrypted communications channel is created. The method comprises: (1) receiving from the client device a request for a network address associated with the target device; (2) determining whether the request transmitted in step (1) is requesting access to a device that accepts an encrypted channel connection with the client device; and (3) in response to determining that the address request in step (2) is requesting access to a device that accepts an encrypted communications channel connection with the client device, providing provisioning information required to initiate the creation of the encrypted communications channel between the client device and the target device such that the encrypted communications channel supports secure audio/video communications transmitted between the two devices.

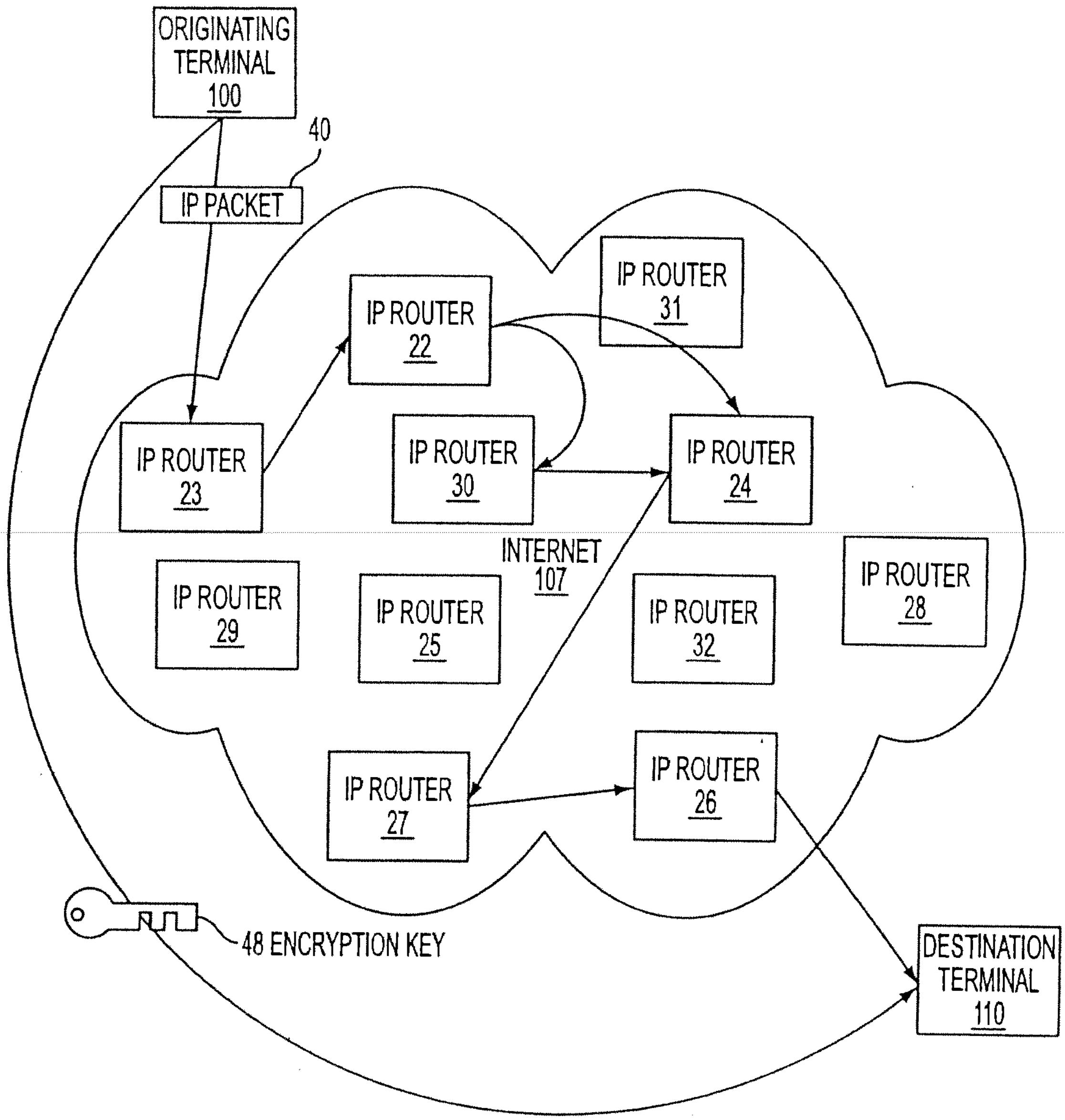
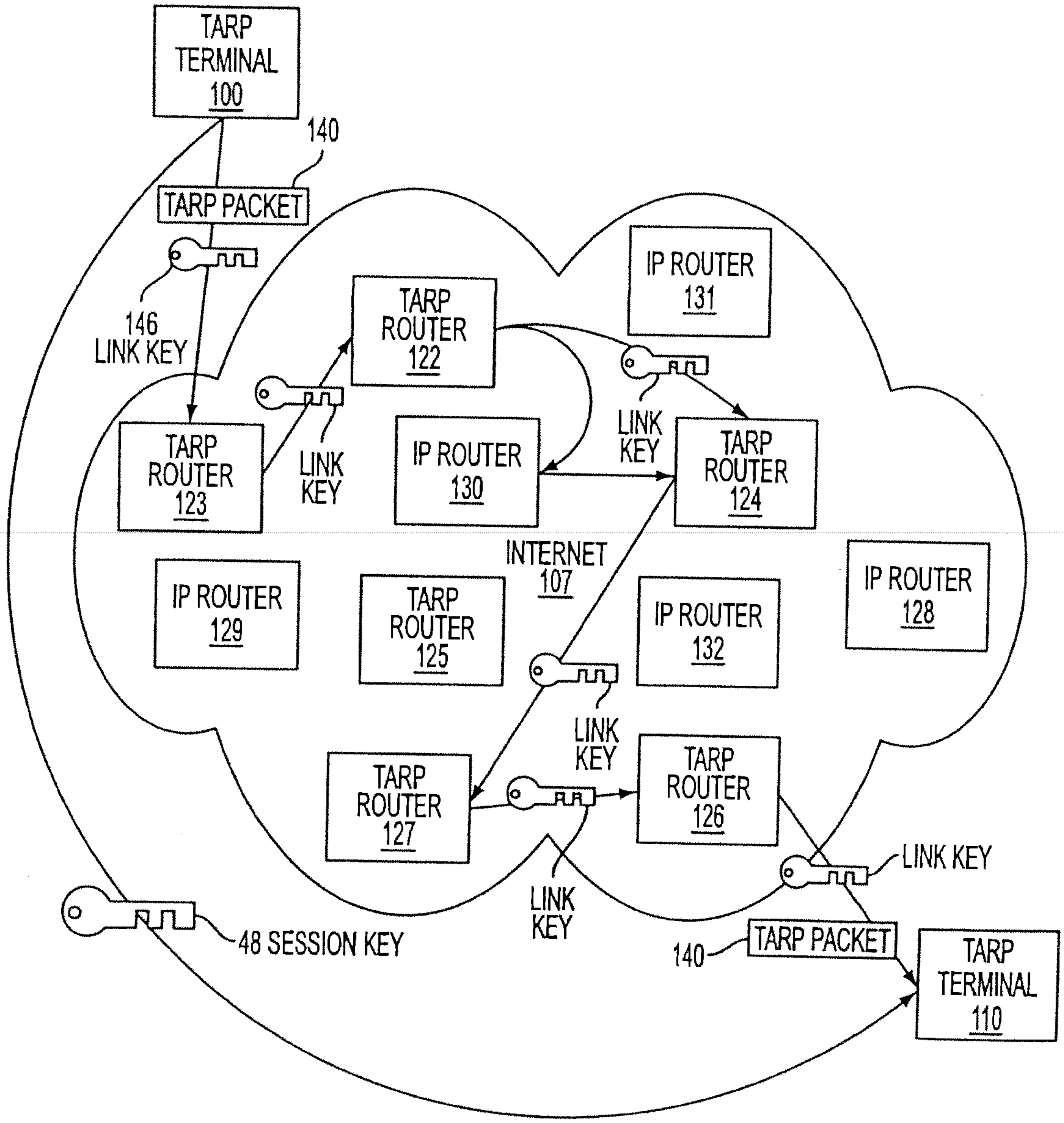
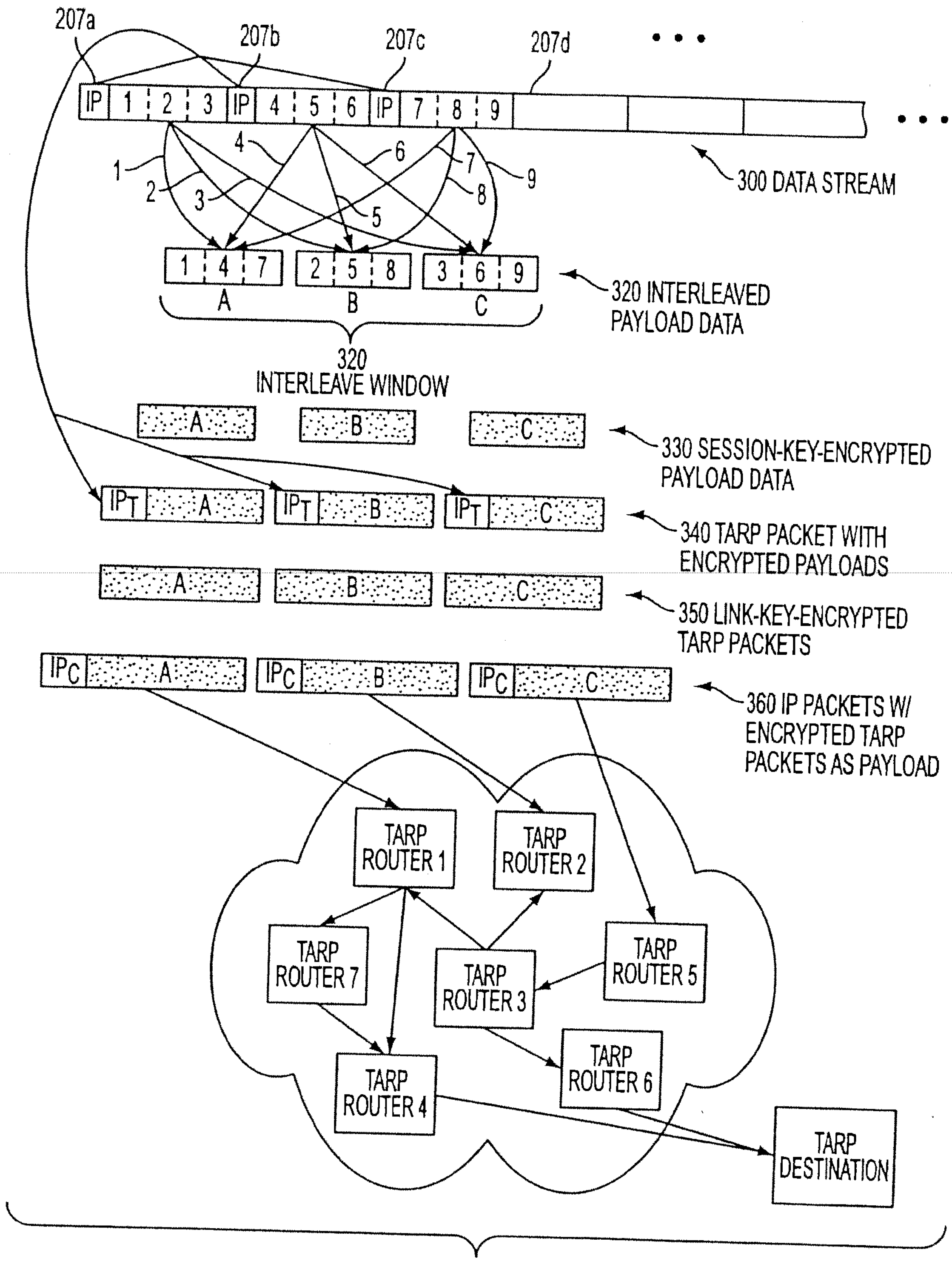

ORIGINATING TERMINAL 100
40
IP PACKET
IP ROUTER 22
IP ROUTER 31
IP ROUTER 23
IP ROUTER 30
IP ROUTER 24
INTERNET 107
IP ROUTER 29
IP ROUTER 25
IP ROUTER 32
IP ROUTER 28
IP ROUTER 27
IP ROUTER 26
48 ENCRYPTION KEY
DESTINATION TERMINAL 110

FIG. 1



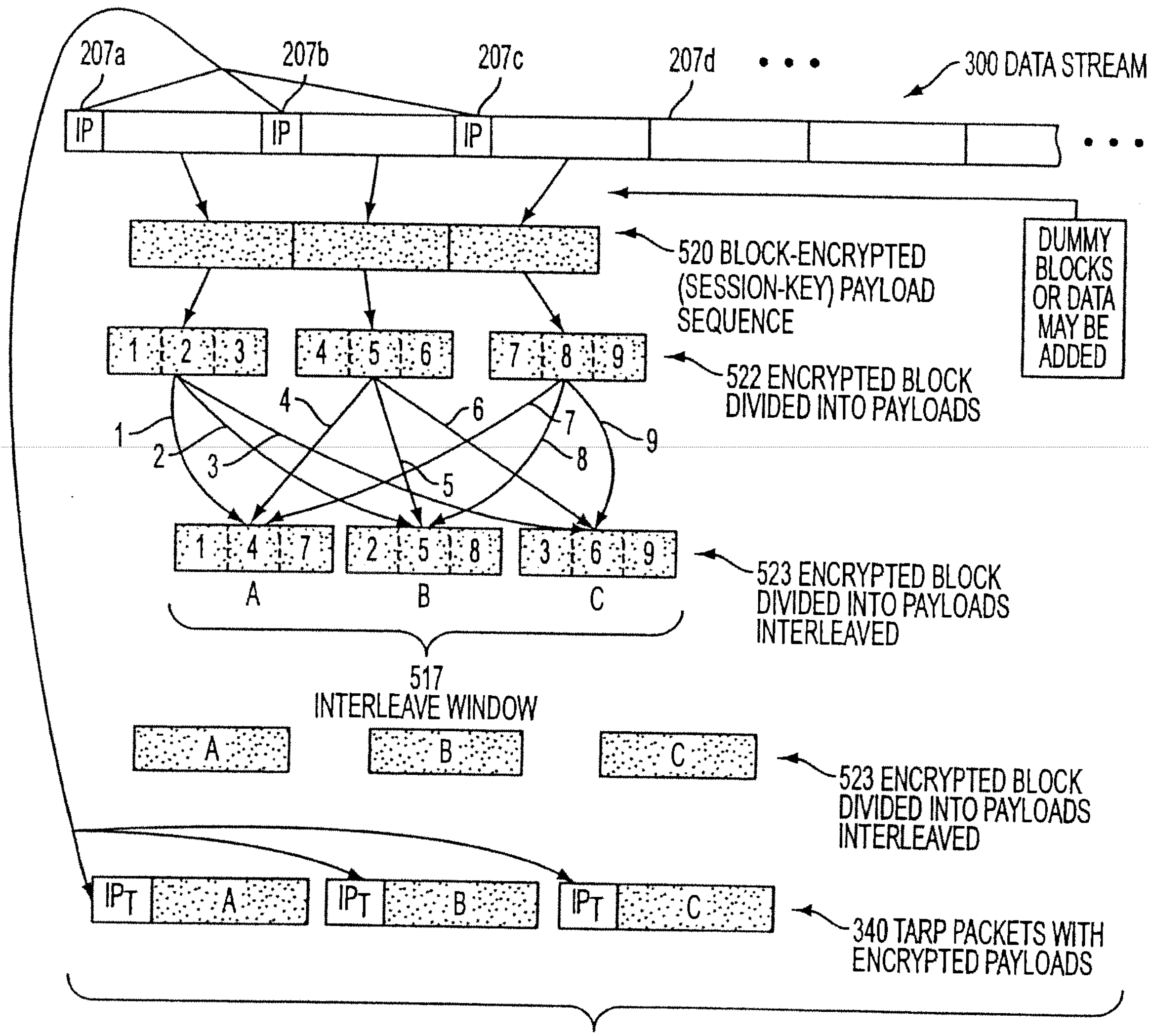
TARP TERMINAL 100
140
TARP PACKET
146 LINK KEY
TARP ROUTER 122
IP ROUTER 131
LINK KEY
TARP ROUTER 123
LINK KEY
IP ROUTER 130
TARP ROUTER 124
INTERNET 107
IP ROUTER 129
TARP ROUTER 125
IP ROUTER 132
IP ROUTER 128
LINK KEY
TARP ROUTER 127
TARP ROUTER 126
LINK KEY
LINK KEY
48 SESSION KEY
140
TARP PACKET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

FIG. 2



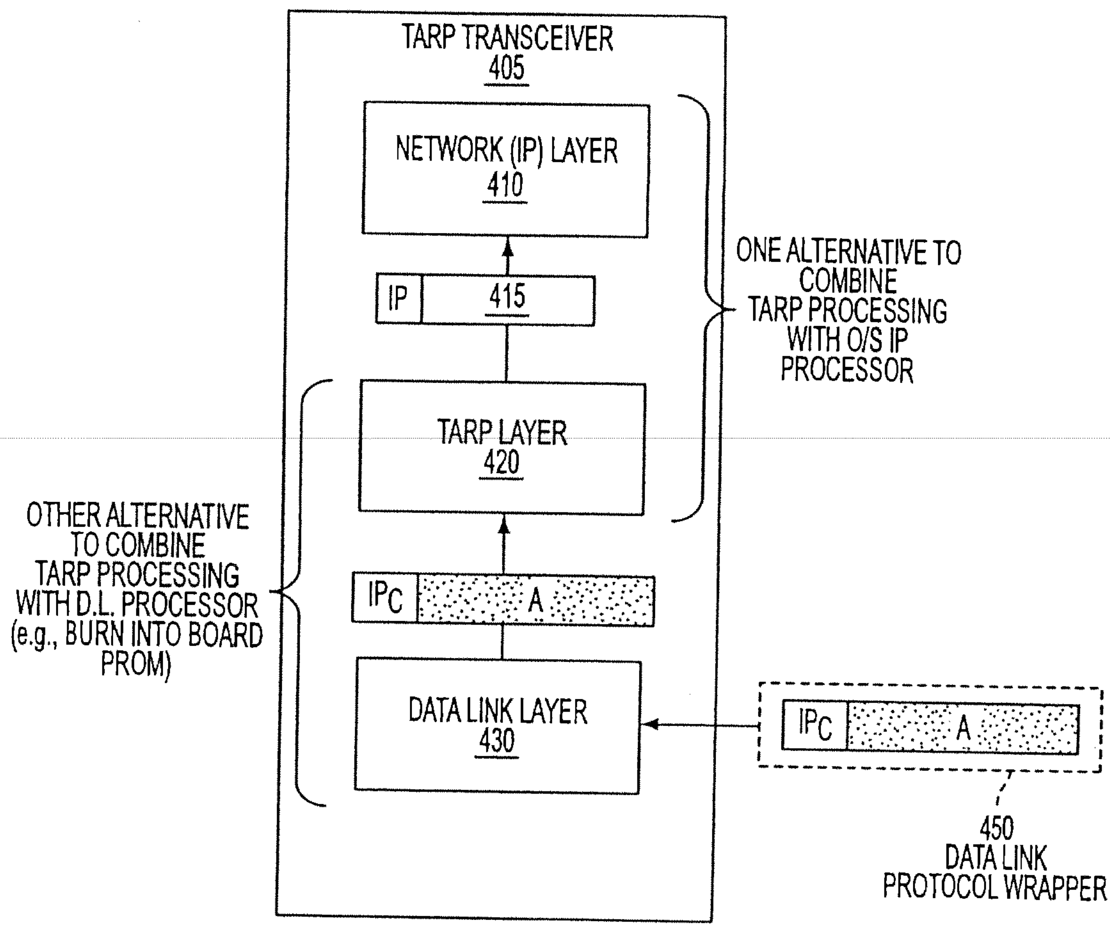
207a
207b
207c
207d
IP
1
2
3
IP
4
5
6
IP
7
8
9
300 DATA STREAM
1
2
3
4
5
6
7
8
9
1
4
7
2
5
8
3
6
9
A
B
C
320 INTERLEAVED PAYLOAD DATA
320 INTERLEAVE WINDOW
A
B
C
330 SESSION-KEY-ENCRYPTED PAYLOAD DATA
IP_T
A
IP_T
B
IP_T
C
340 TARP PACKET WITH ENCRYPTED PAYLOADS
A
B
C
350 LINK-KEY-ENCRYPTED TARP PACKETS
IP_C
A
IP_C
B
IP_C
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
DUMMY BLOCKS OR DATA MAY BE ADDED
520 BLOCK-ENCRYPTED (SESSION-KEY) PAYLOAD SEQUENCE
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

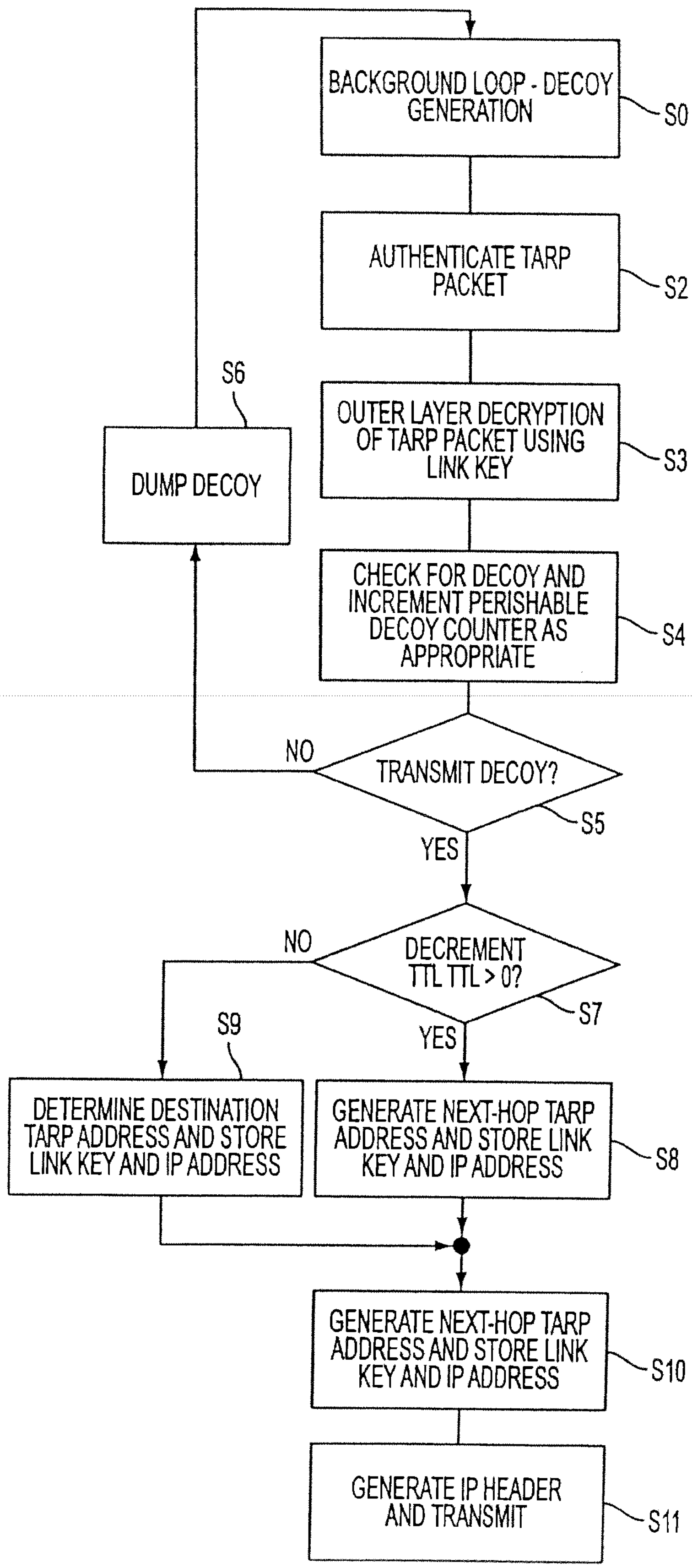

BACKGROUND LOOP - DECOY GENERATION
S0
AUTHENTICATE TARP PACKET
S2
OUTER LAYER DECRYPTION OF TARP PACKET USING LINK KEY
S3
CHECK FOR DECOY AND INCREMENT PERISHABLE DECOY COUNTER AS APPROPRIATE
S4
S6
DUMP DECOY
NO
TRANSMIT DECOY?
S5
YES
NO
DECREMENT TTL TTL > 0?
S7
YES
S9
DETERMINE DESTINATION TARP ADDRESS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

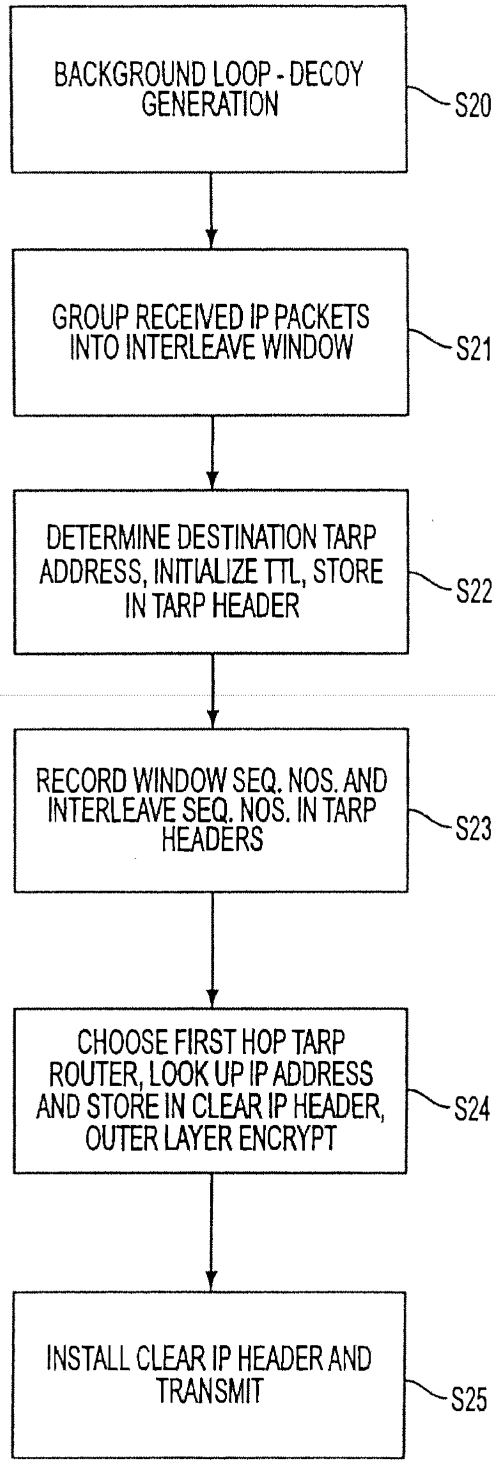

BACKGROUND LOOP - DECOY GENERATION
S20
GROUP RECEIVED IP PACKETS INTO INTERLEAVE WINDOW
S21
DETERMINE DESTINATION TARP ADDRESS, INITIALIZE TTL, STORE IN TARP HEADER
S22
RECORD WINDOW SEQ. NOS. AND INTERLEAVE SEQ. NOS. IN TARP HEADERS
S23
CHOOSE FIRST HOP TARP ROUTER, LOOK UP IP ADDRESS AND STORE IN CLEAR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

FIG. 6

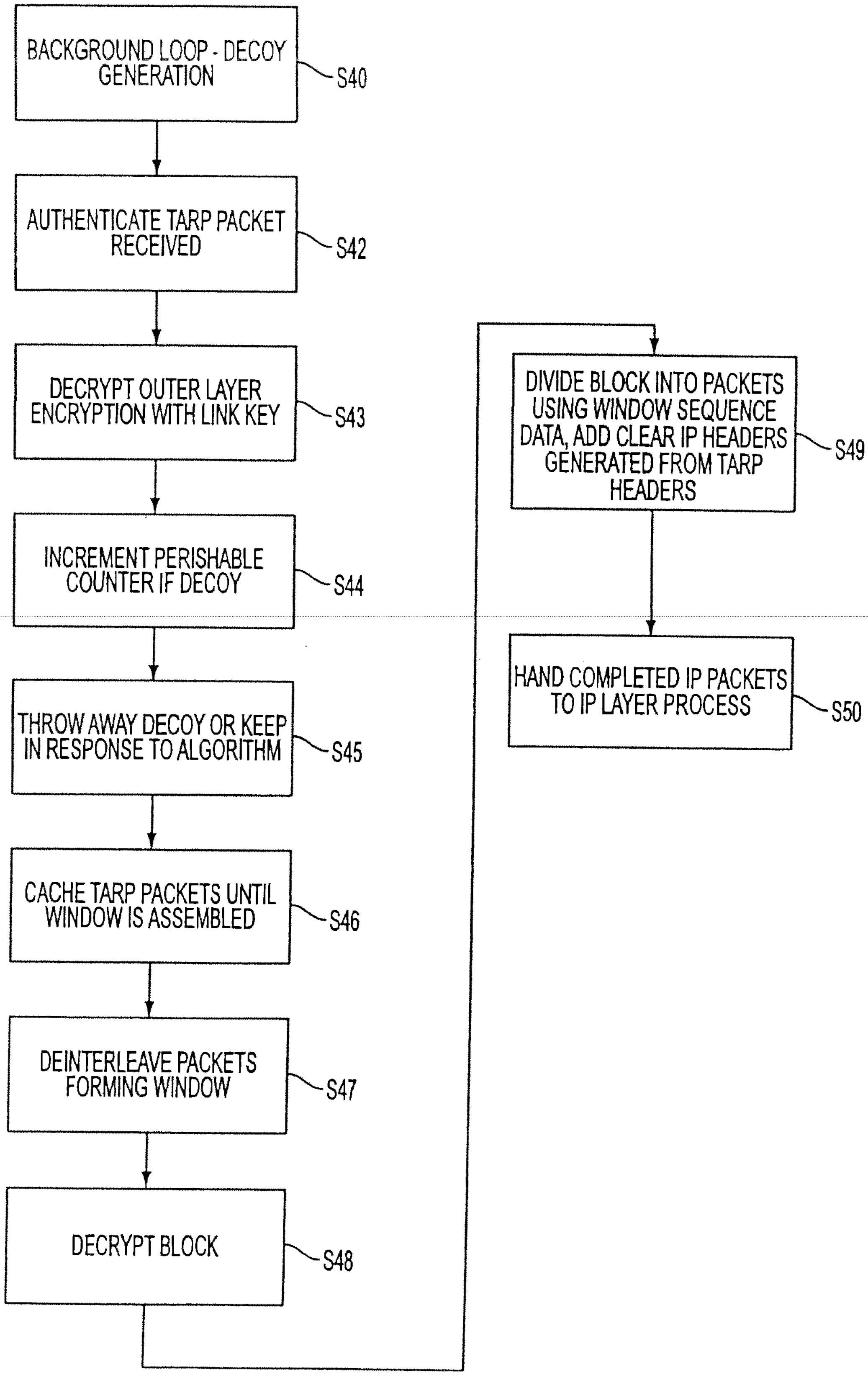

BACKGROUND LOOP - DECOY GENERATION
S40
AUTHENTICATE TARP PACKET RECEIVED
S42
DECRYPT OUTER LAYER ENCRYPTION WITH LINK KEY
S43
INCREMENT PERISHABLE COUNTER IF DECOY
S44
THROW AWAY DECOY OR KEEP IN RESPONSE TO ALGORITHM
S45
CACHE TARP PACKETS UNTIL WINDOW IS ASSEMBLED
S46
DEINTERLEAVE PACKETS FORMING WINDOW
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

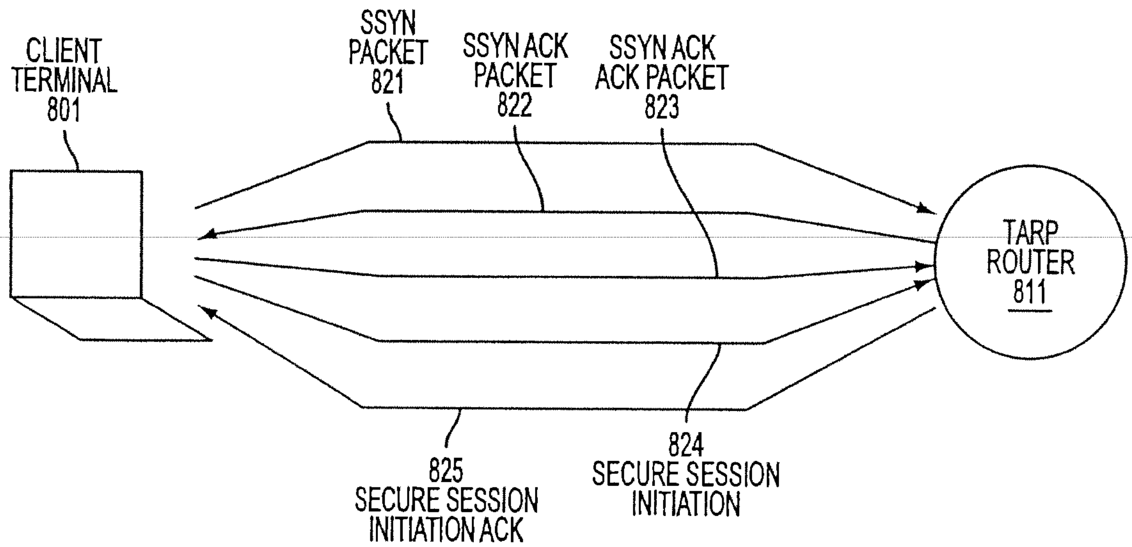
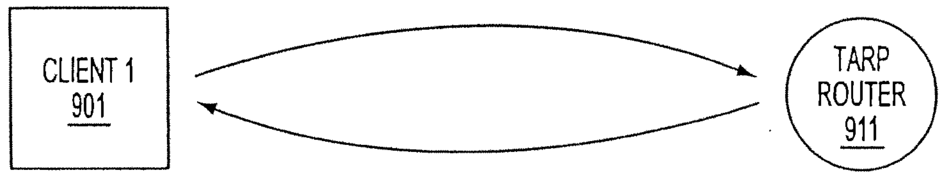

CLIENT
TERMINAL
801
SSYN
PACKET
821
SSYN ACK
PACKET
822
SSYN ACK
ACK PACKET
823
TARP
ROUTER
811
825
SECURE SESSION
INITIATION ACK
824
SECURE SESSION
INITIATION

FIG. 8



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

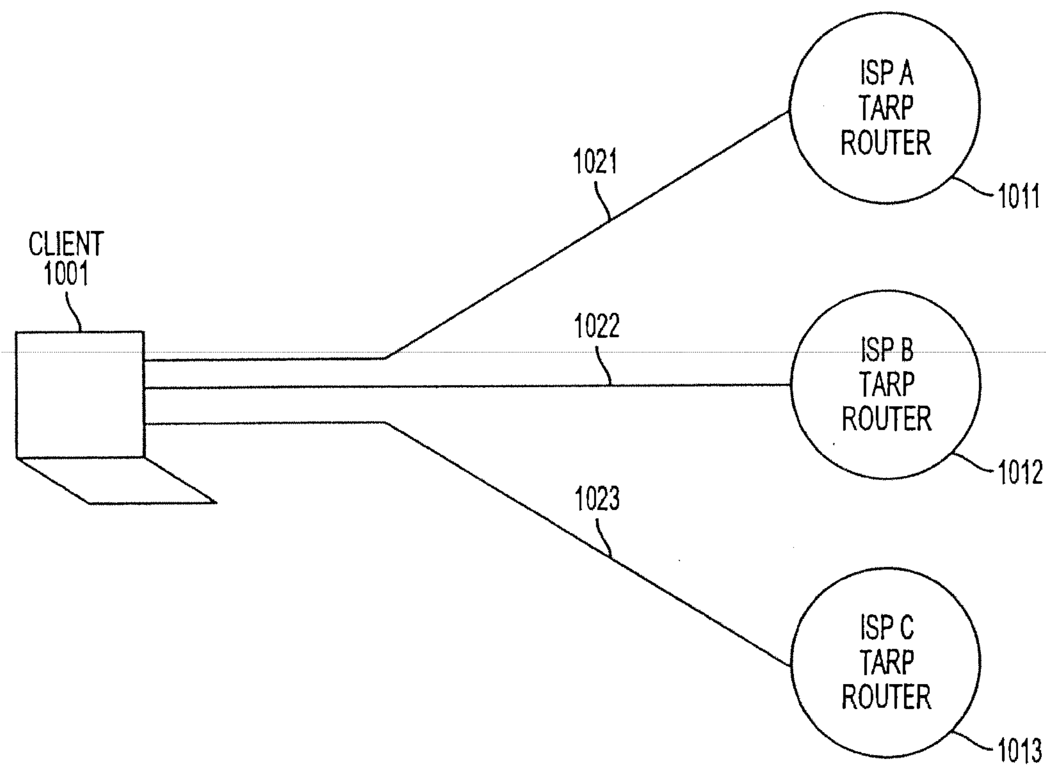

ISP A
TARP
ROUTER
1021
1011
CLIENT
1001
1022
ISP B
TARP
ROUTER
1012
1023
ISP C
TARP
ROUTER
1013

FIG. 10

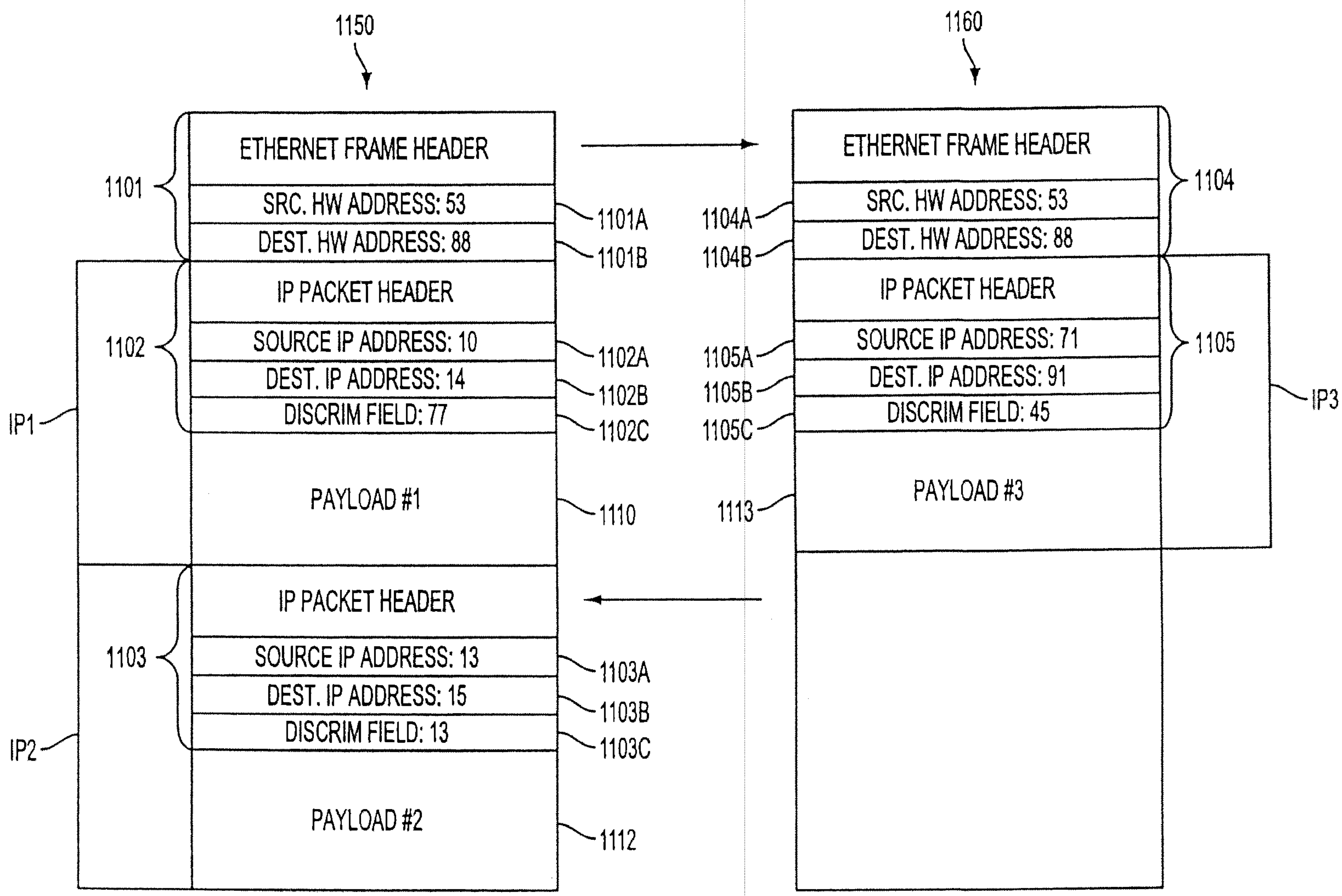

1150
1160
ETHERNET FRAME HEADER
SRC. HW ADDRESS: 53
DEST. HW ADDRESS: 88
IP PACKET HEADER
SOURCE IP ADDRESS: 10
DEST. IP ADDRESS: 14
DISCRIM FIELD: 77
PAYLOAD #1
IP PACKET HEADER
SOURCE IP ADDRESS: 13
DEST. IP ADDRESS: 15
DISCRIM FIELD: 13
PAYLOAD #2
ETHERNET FRAME HEADER
SRC. HW ADDRESS: 53
DEST. HW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

FIG. 11

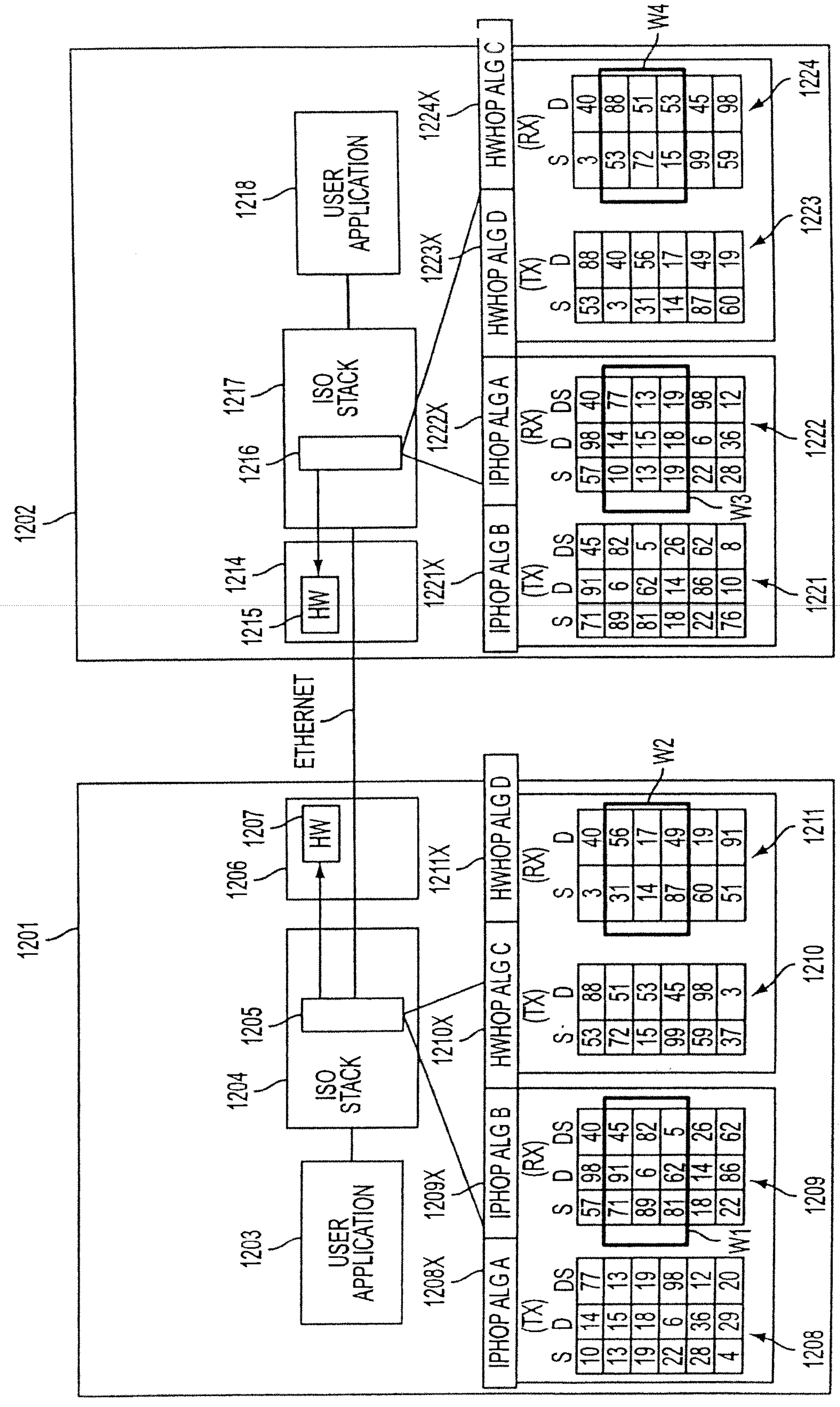

1201
1202
1203
USER APPLICATION
1204
ISO STACK
1205
1206
1207
HW
1208X
IPHOP ALG A
1209X
IPHOP ALG B
1210X
HWHOP ALG C
1211X
HWHOP ALG D
1208
1209
1210
1211
W1
W2
ETHERNET
1214
1215
HW
1216
1217
ISO STACK
1218
USER APPLICATION
1221X
IPHOP ALG B
1222X
IPHOP ALG A
1223X
HWHOP ALG D
1224X
HWHOP ALG C
1221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

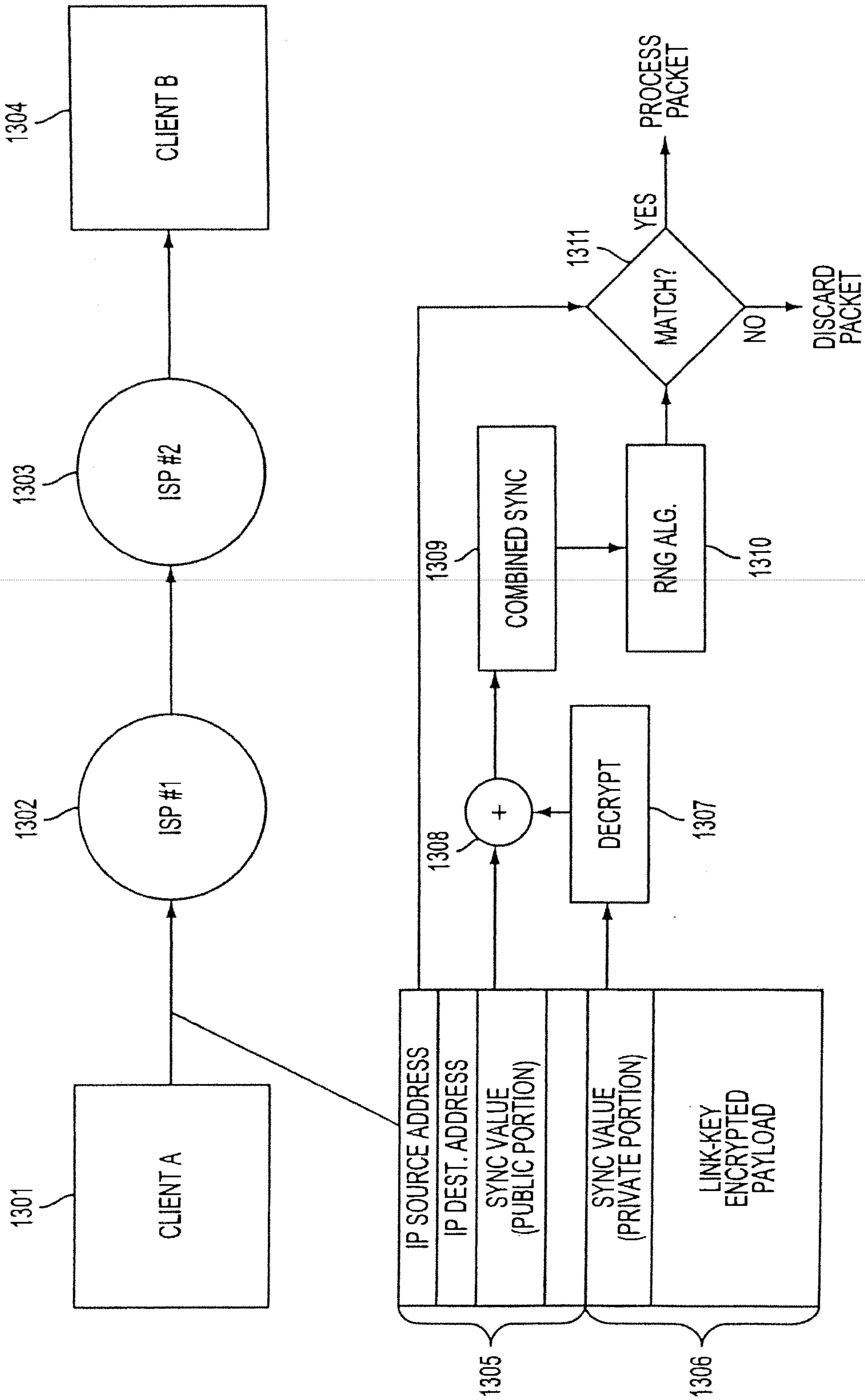

1301
CLIENT A
1302
ISP #1
1303
ISP #2
1304
CLIENT B
IP SOURCE ADDRESS
IP DEST. ADDRESS
SYNC VALUE (PUBLIC PORTION)
SYNC VALUE (PRIVATE PORTION)
LINK-KEY ENCRYPTED PAYLOAD
1305
1306
1307
DECRYPT
1308
+
1309
COMBINED SYNC
1310
RNG ALG.
1311
MATCH?
YES
PROCESS PACKET
NO
DISCARD PACKET

FIG. 13

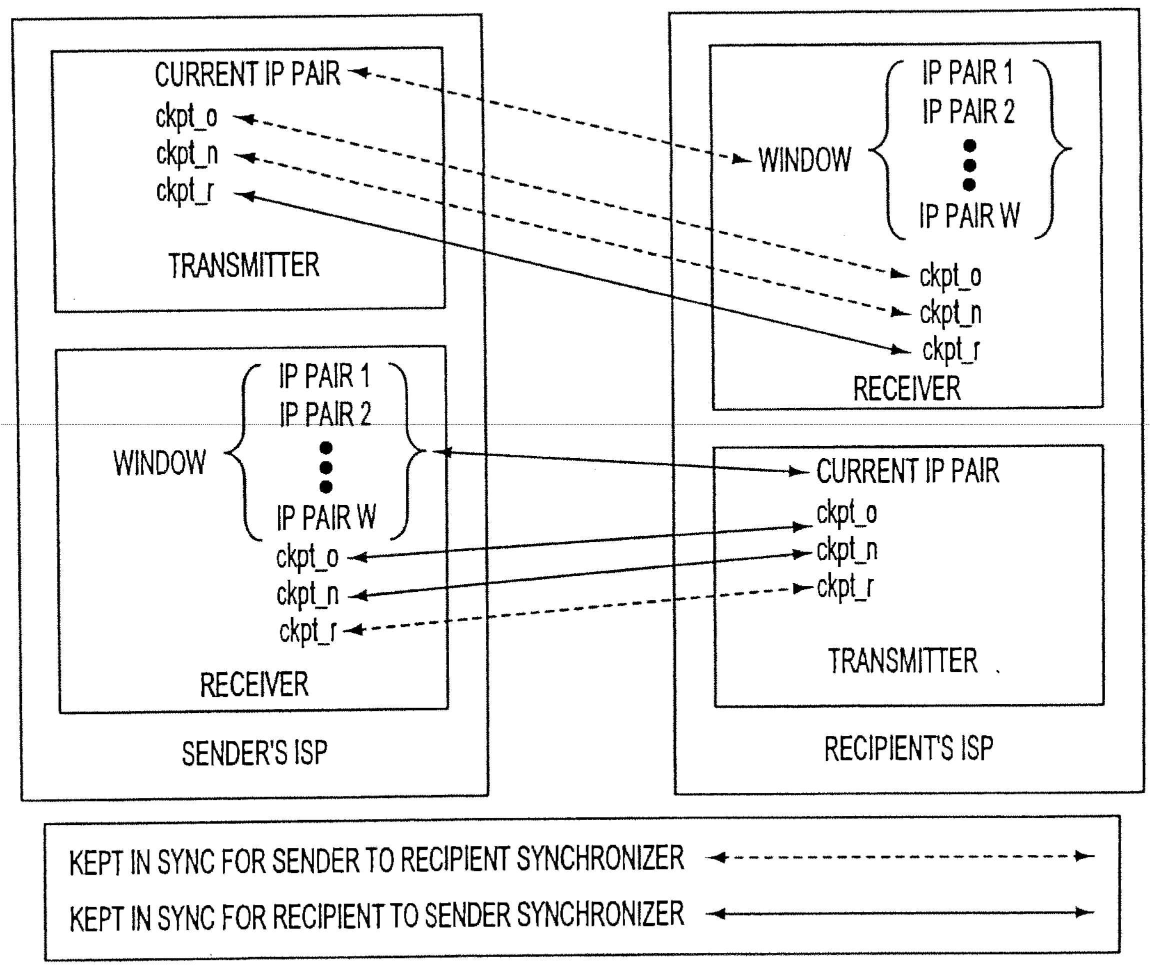

CURRENT IP PAIR
ckpt_o
ckpt_n
ckpt_r
TRANSMITTER
WINDOW
IP PAIR 1
IP PAIR 2
IP PAIR W
ckpt_o
ckpt_n
ckpt_r
RECEIVER
SENDER'S ISP
WINDOW
IP PAIR 1
IP PAIR 2
IP PAIR W
ckpt_o
ckpt_n
ckpt_r
RECEIVER
CURRENT IP PAIR
ckpt_o
ckpt_n
ckpt_r
TRANSMITTER
RECIPIENT'S ISP
KEPT IN SYNC FOR SENDER TO RECIPIENT SYNCHRONIZER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

FIG. 14

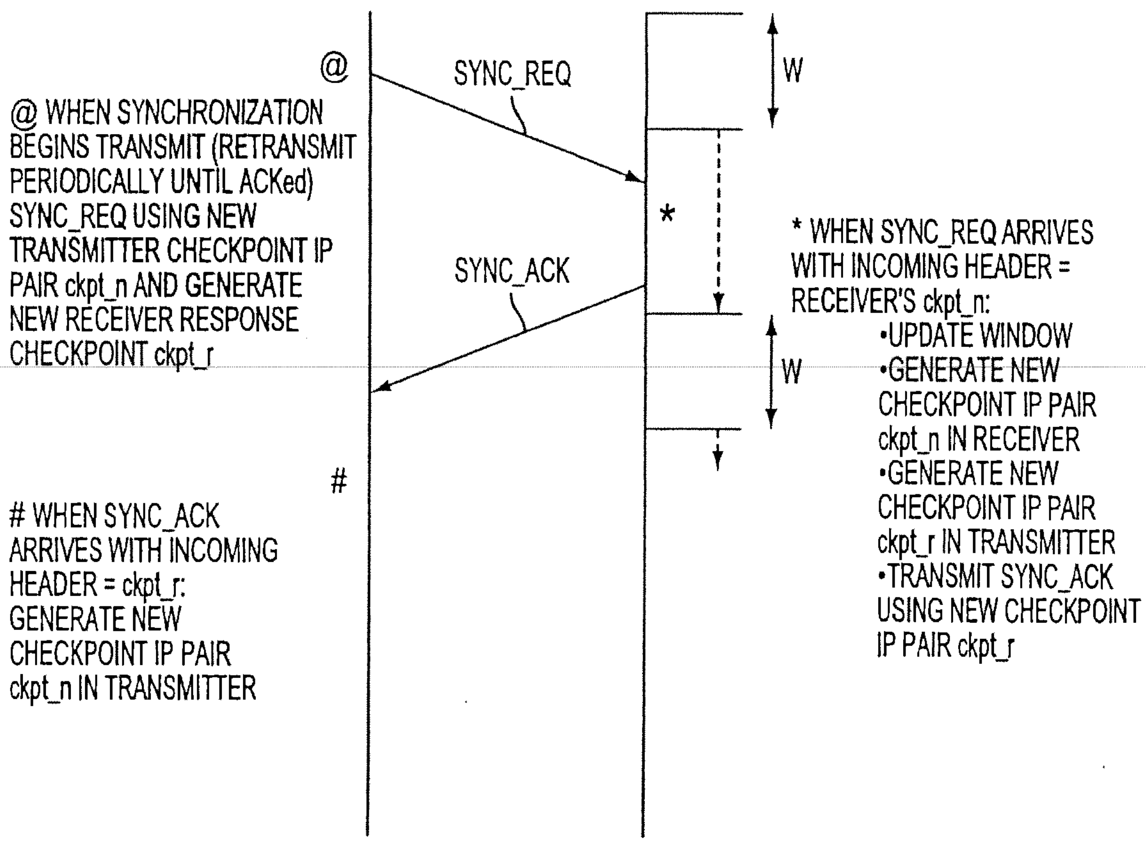

@
SYNC_REQ
W
@ WHEN SYNCHRONIZATION BEGINS TRANSMIT (RETRANSMIT PERIODICALLY UNTIL ACKed) SYNC_REQ USING NEW TRANSMITTER CHECKPOINT IP PAIR ckpt_n AND GENERATE NEW RECEIVER RESPONSE CHECKPOINT ckpt_r
*
SYNC_ACK
* WHEN SYNC_REQ ARRIVES WITH INCOMING HEADER = RECEIVER'S ckpt_n:
•UPDATE WINDOW
•GENERATE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

FIG. 15

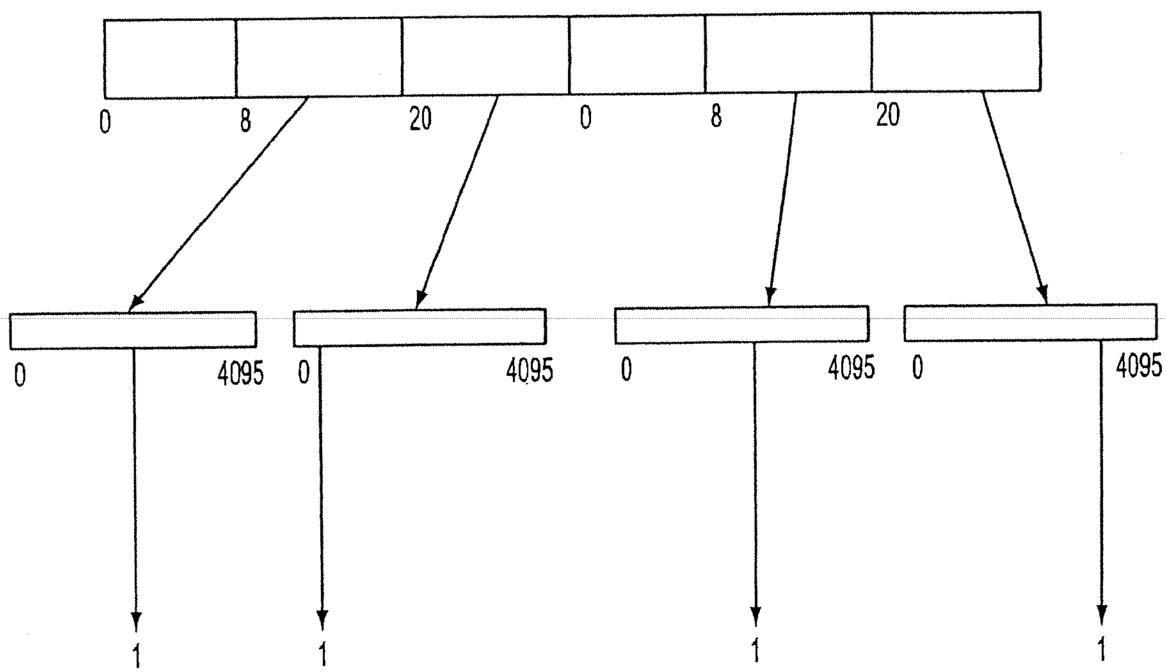


FIG. 16

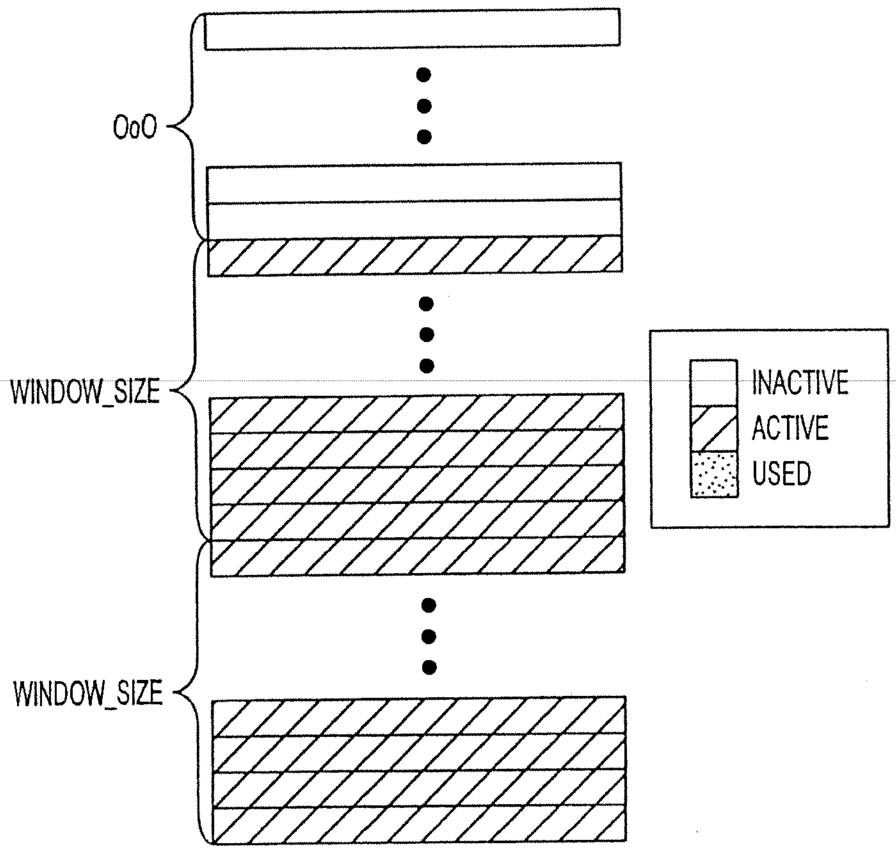


FIG. 17

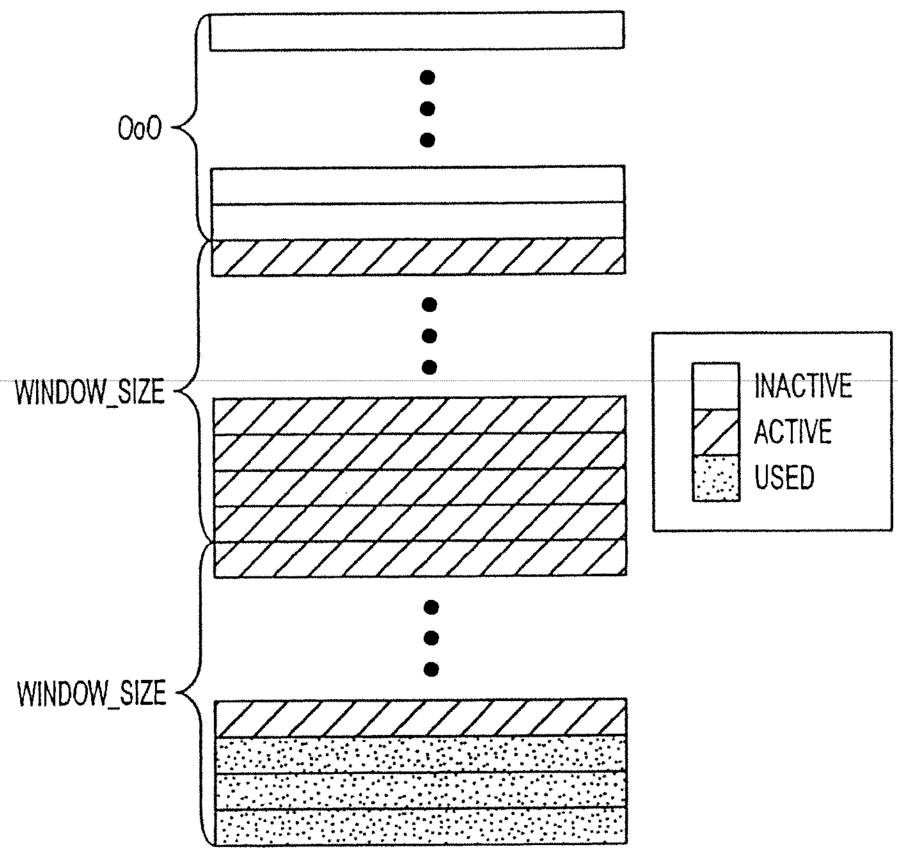


FIG. 18

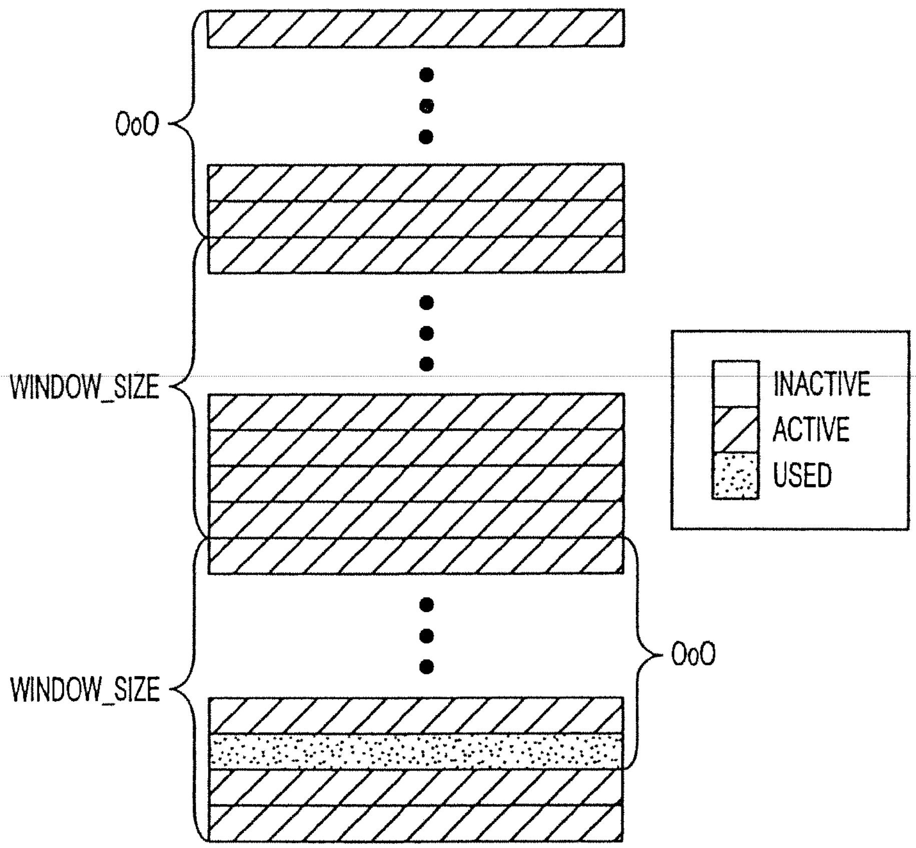
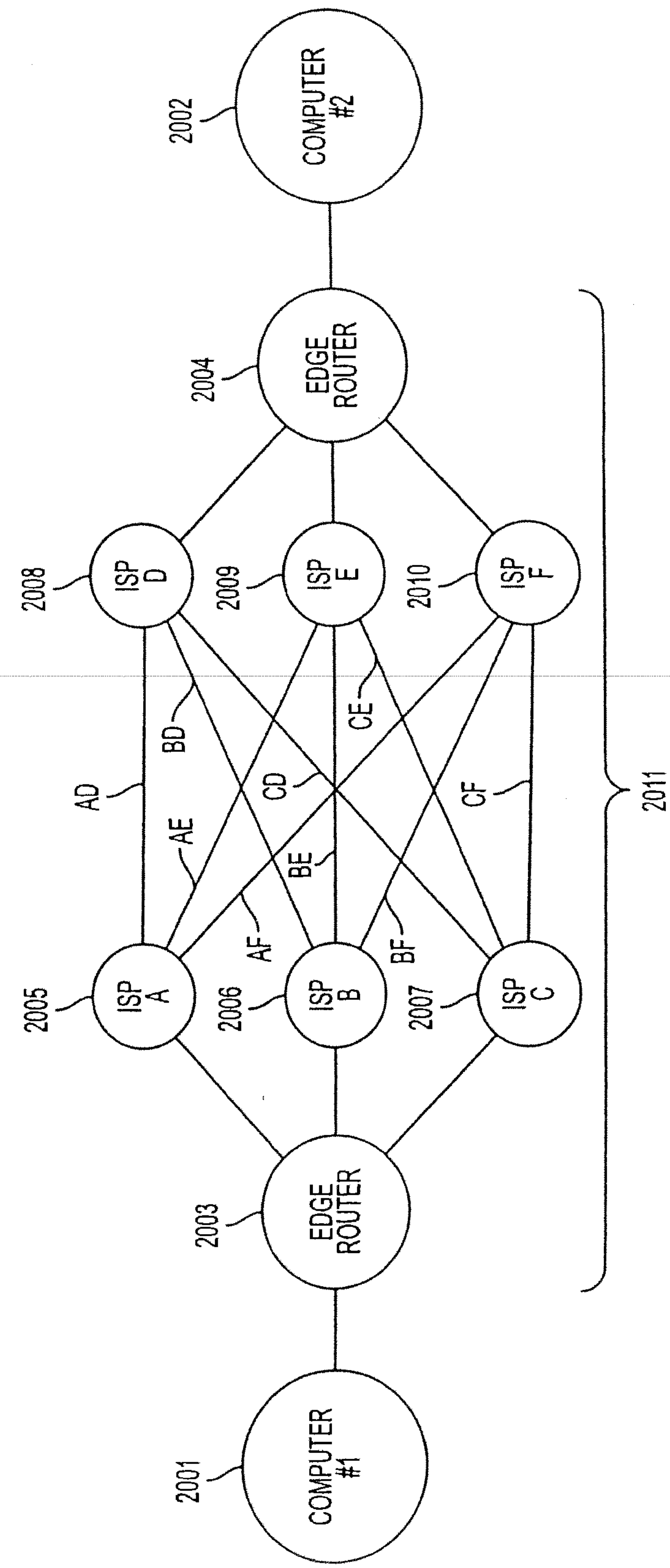


FIG. 19



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

FIG. 20

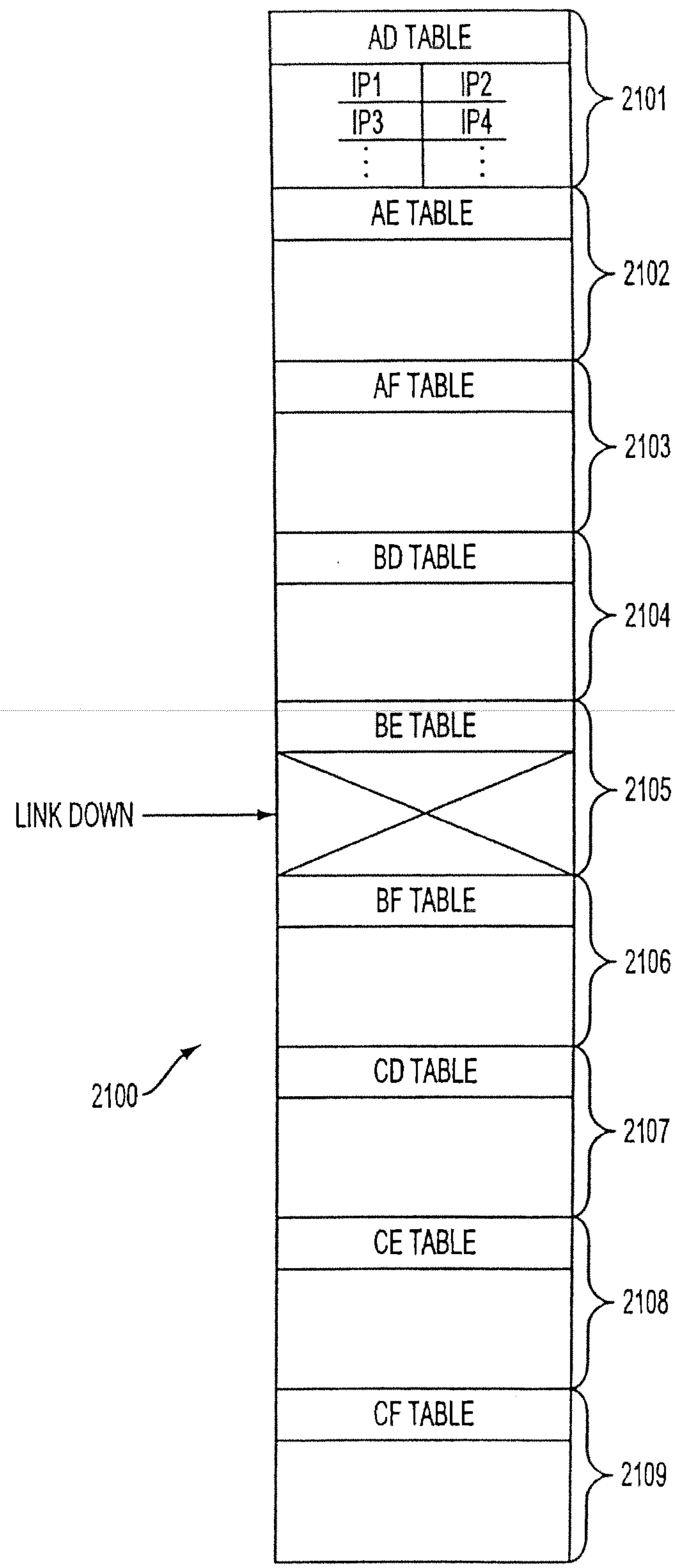

AD TABLE
IP1
IP2
IP3
IP4
AE TABLE
AF TABLE
BD TABLE
BE TABLE
LINK DOWN
BF TABLE
CD TABLE
CE TABLE
CF TABLE
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109

FIG. 21

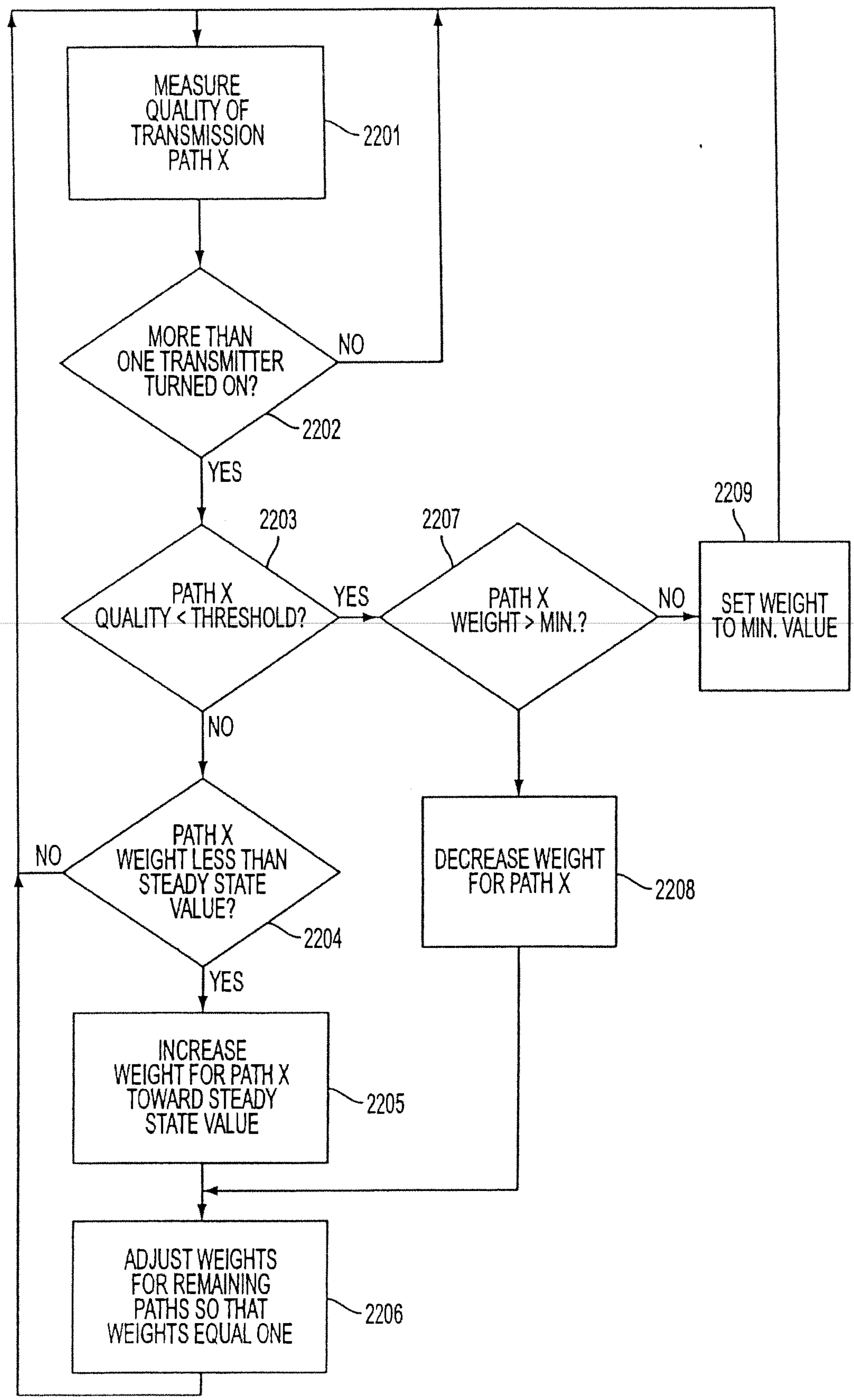

MEASURE QUALITY OF TRANSMISSION PATH X
2201
MORE THAN ONE TRANSMITTER TURNED ON?
NO
2202
YES
2203
PATH X QUALITY < THRESHOLD?
YES
2207
PATH X WEIGHT > MIN.?
NO
2209
SET WEIGHT TO MIN. VALUE
NO
PATH X WEIGHT LESS THAN STEADY STATE VALUE?
NO
2204
YES
DECREASE WEIGHT FOR PATH X
2208
INCREASE WEIGHT FOR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

FIG. 22A

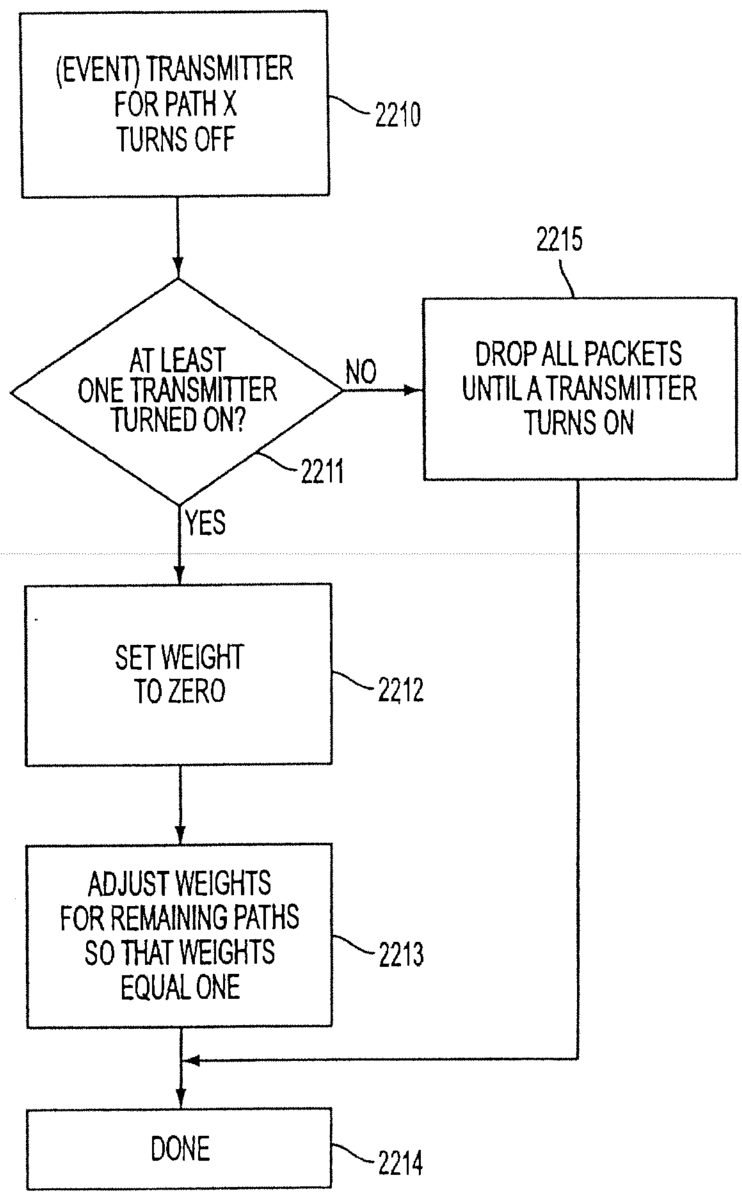

(EVENT) TRANSMITTER FOR PATH X TURNS OFF
2210
AT LEAST ONE TRANSMITTER TURNED ON?
2211
NO
YES
2215
DROP ALL PACKETS UNTIL A TRANSMITTER TURNS ON
SET WEIGHT TO ZERO
2212
ADJUST WEIGHTS FOR REMAINING PATHS SO THAT WEIGHTS EQUAL ONE
2213
DONE
2214

FIG. 22B

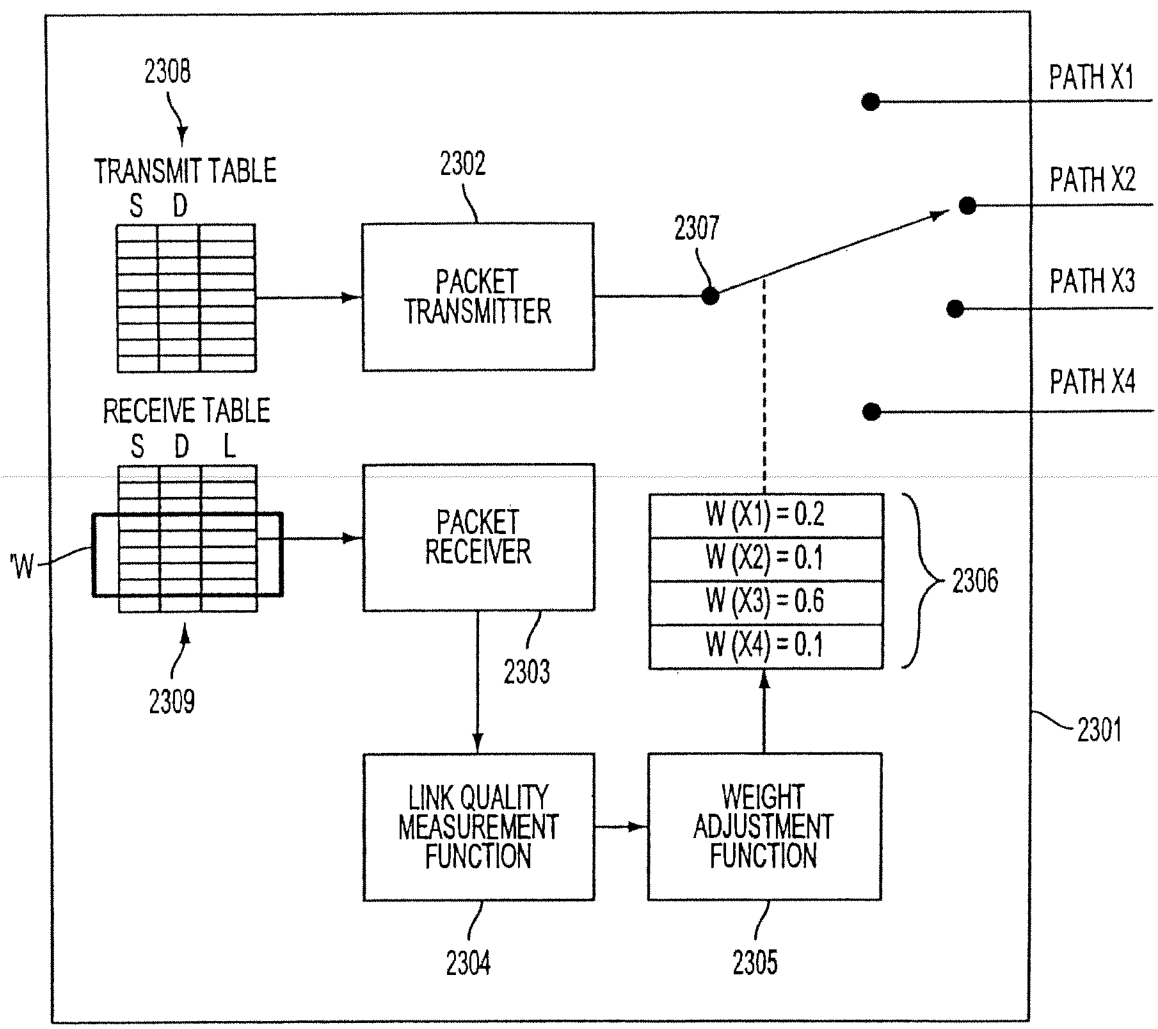

2308
TRANSMIT TABLE
S D
2302
PACKET TRANSMITTER
2307
PATH X1
PATH X2
PATH X3
PATH X4
RECEIVE TABLE
S D L
'W
PACKET RECEIVER
W (X1) = 0.2
W (X2) = 0.1
W (X3) = 0.6
W (X4) = 0.1
2306
2309
2303
2301
LINK QUALITY MEASUREMENT FUNCTION
WEIGHT ADJUSTMENT FUNCTION
2304
2305

FIG. 23

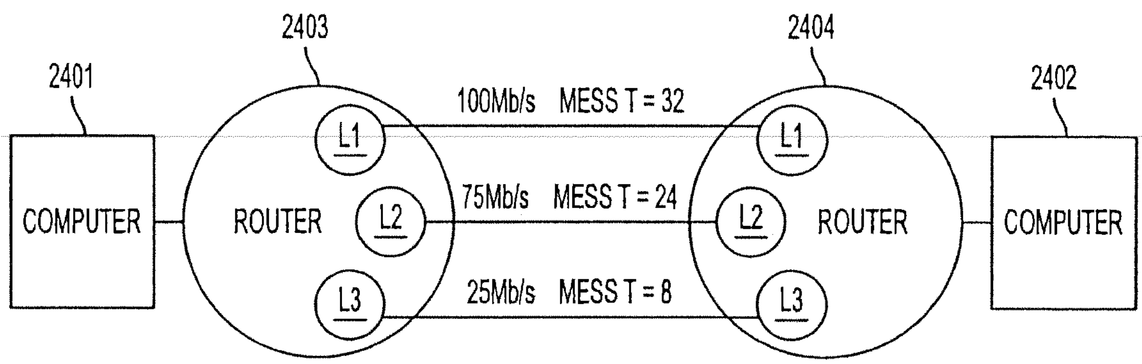

2403
2404
2401
2402
100Mb/s MESS T = 32
75Mb/s MESS T = 24
25Mb/s MESS T = 8
COMPUTER
ROUTER
L1
L2
L3
L1
L2
L3
ROUTER
COMPUTER

FIG. 24

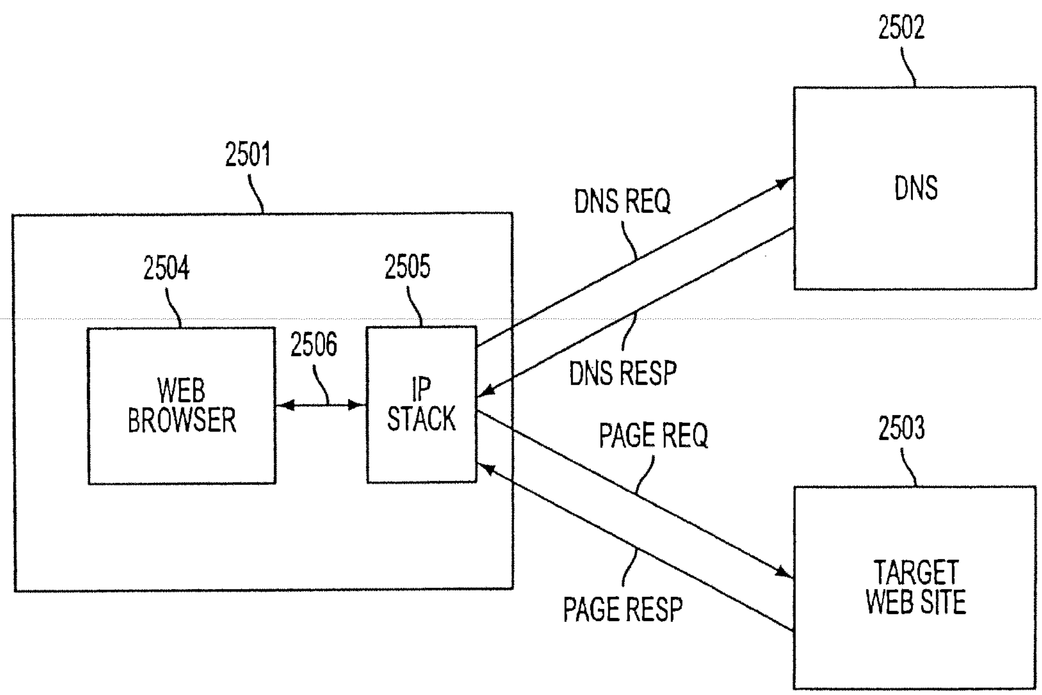


FIG. 25
(PRIOR ART)

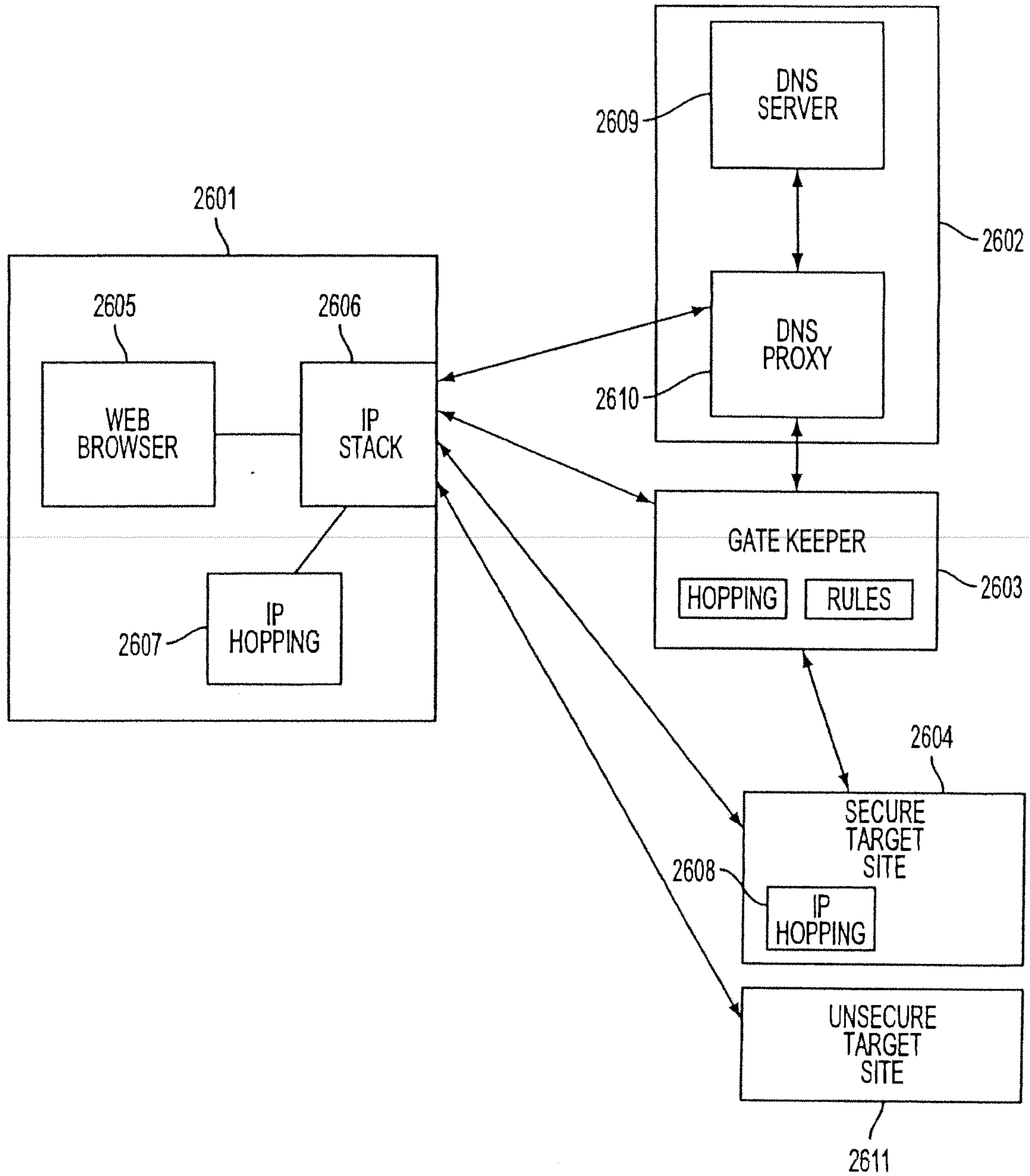

2601
2605
2606
WEB BROWSER
IP STACK
2607
IP HOPPING
2609
DNS SERVER
2602
2610
DNS PROXY
GATE KEEPER
HOPPING
RULES
2603
2604
SECURE TARGET SITE
2608
IP HOPPING
UNSECURE TARGET SITE
2611

FIG. 26

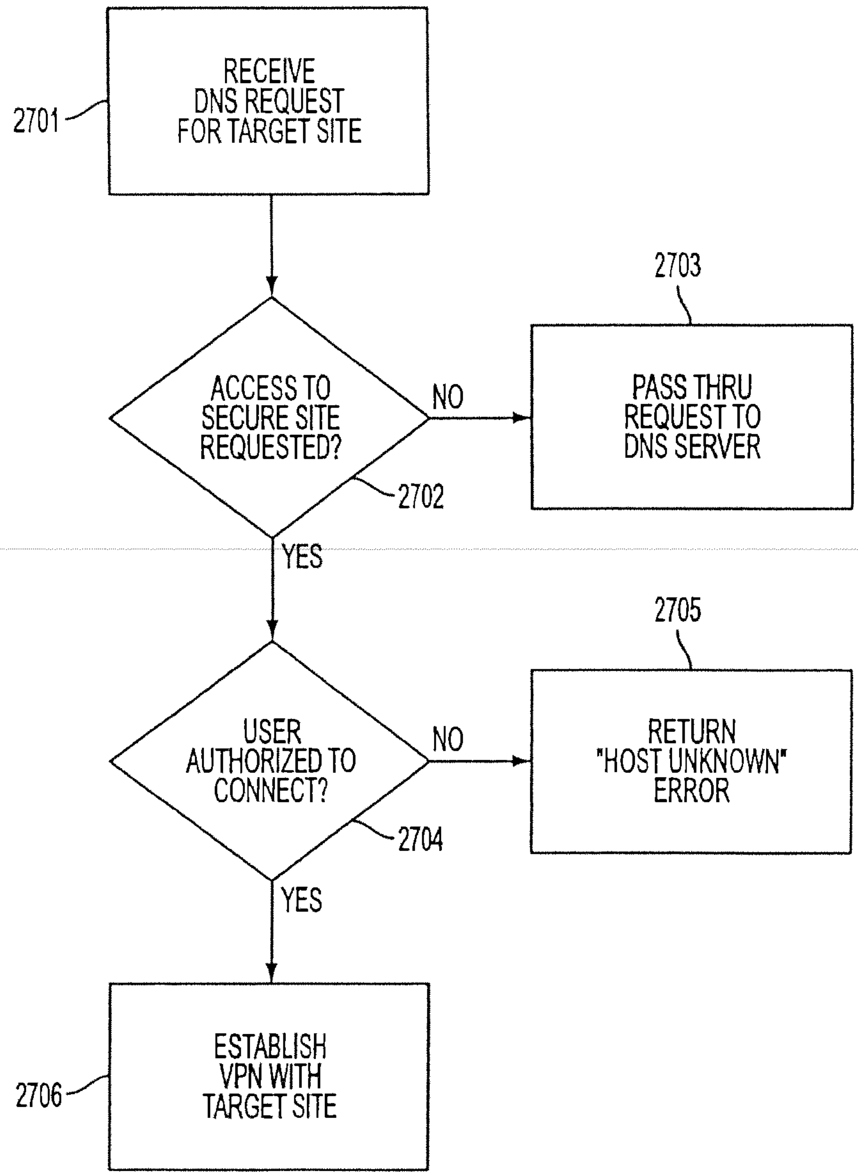

RECEIVE
DNS REQUEST
FOR TARGET SITE
2701
ACCESS TO
SECURE SITE
REQUESTED?
2702
NO
PASS THRU
REQUEST TO
DNS SERVER
2703
YES
USER
AUTHORIZED TO
CONNECT?
2704
NO
RETURN
"HOST UNKNOWN"
ERROR
2705
YES
ESTABLISH
VPN WITH
TARGET SITE
2706

FIG. 27

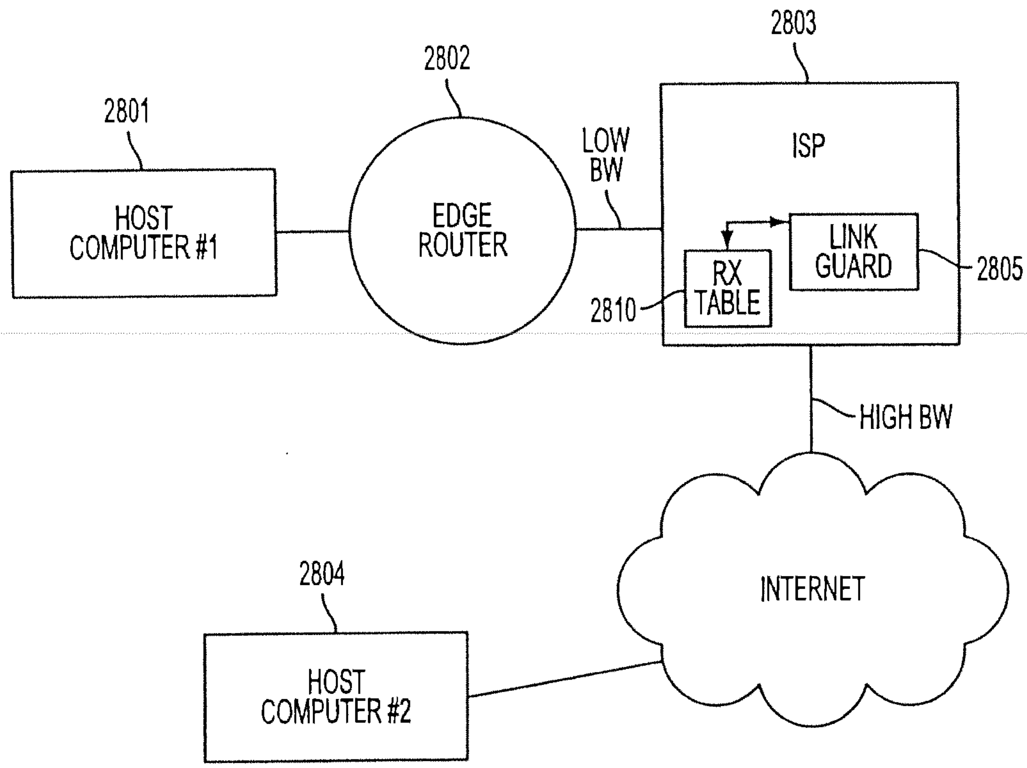
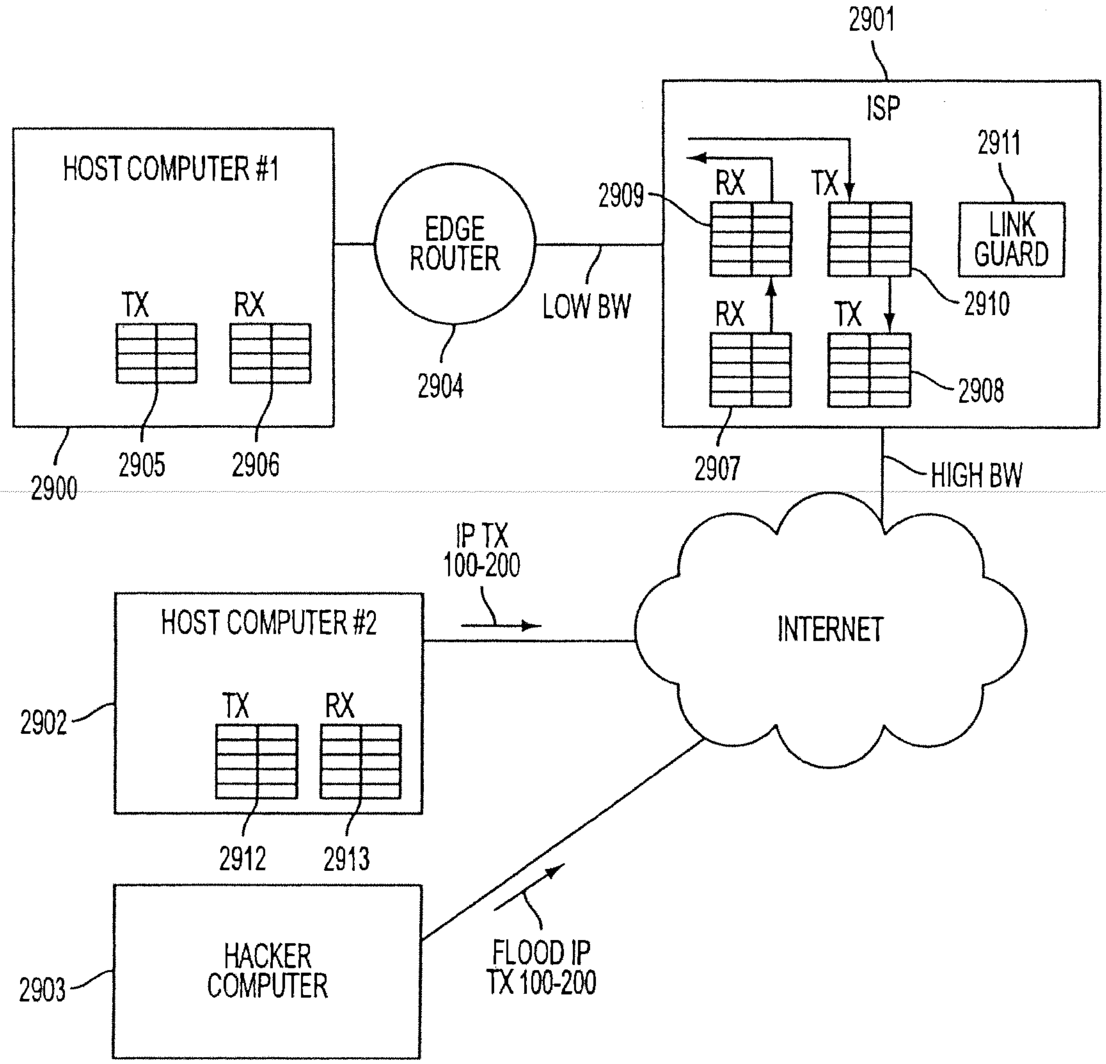
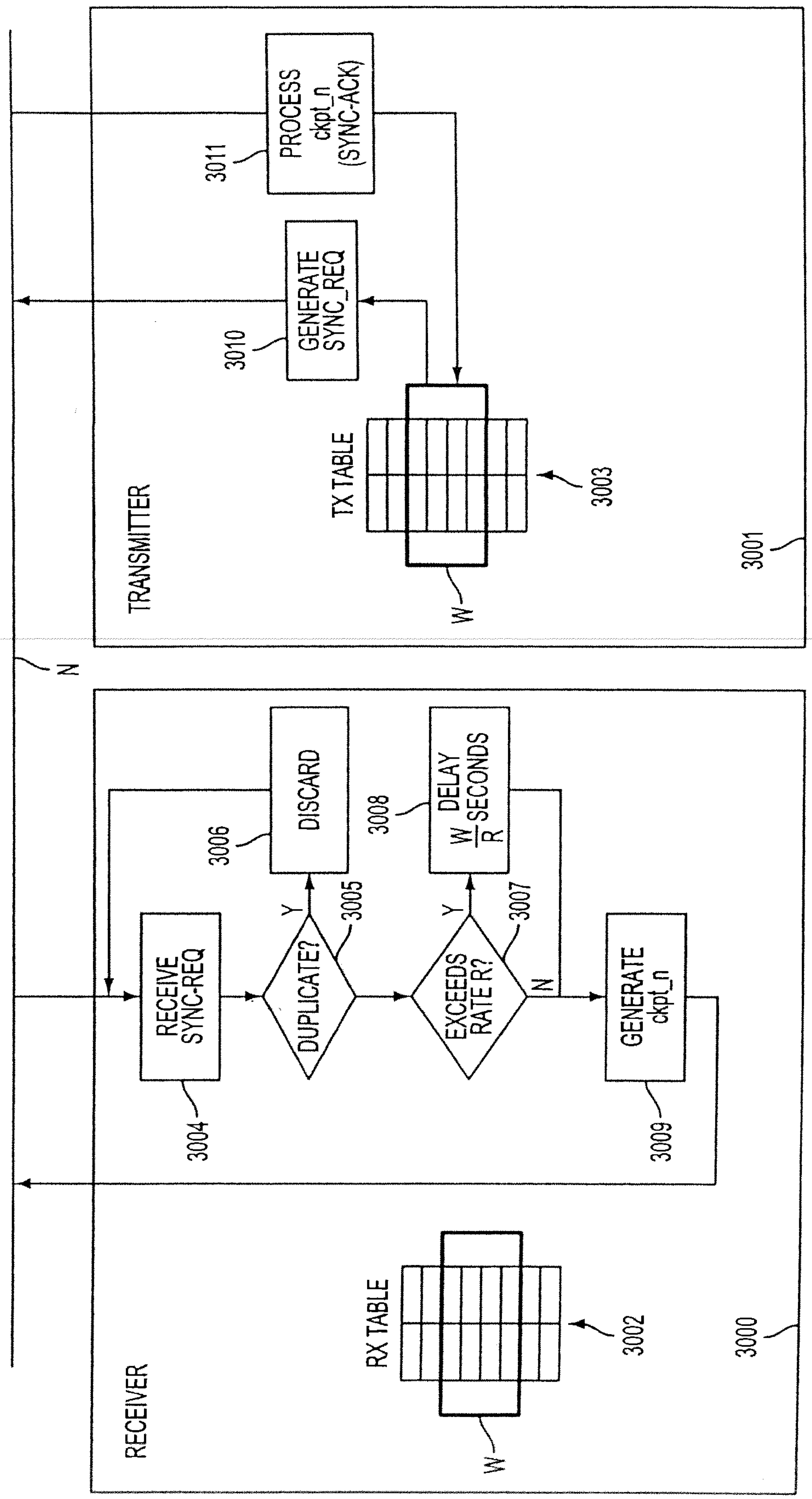

2801
HOST
COMPUTER #1
2802
EDGE
ROUTER
LOW
BW
2803
ISP
RX
TABLE
LINK
GUARD
2810
2805
HIGH BW
INTERNET
2804
HOST
COMPUTER #2

FIG. 28



2901
ISP
2911
LINK GUARD
HOST COMPUTER #1
EDGE ROUTER
2909
RX
TX
RX
TX
2910
2908
LOW BW
2904
TX
RX
2900
2905
2906
2907
HIGH BW
IP TX 100-200
HOST COMPUTER #2
INTERNET
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 $\frac{W}{R}$ SECONDS
3008
GENERATE ckpt_n
3009
RX TABLE
3002
W
3000

FIG. 30

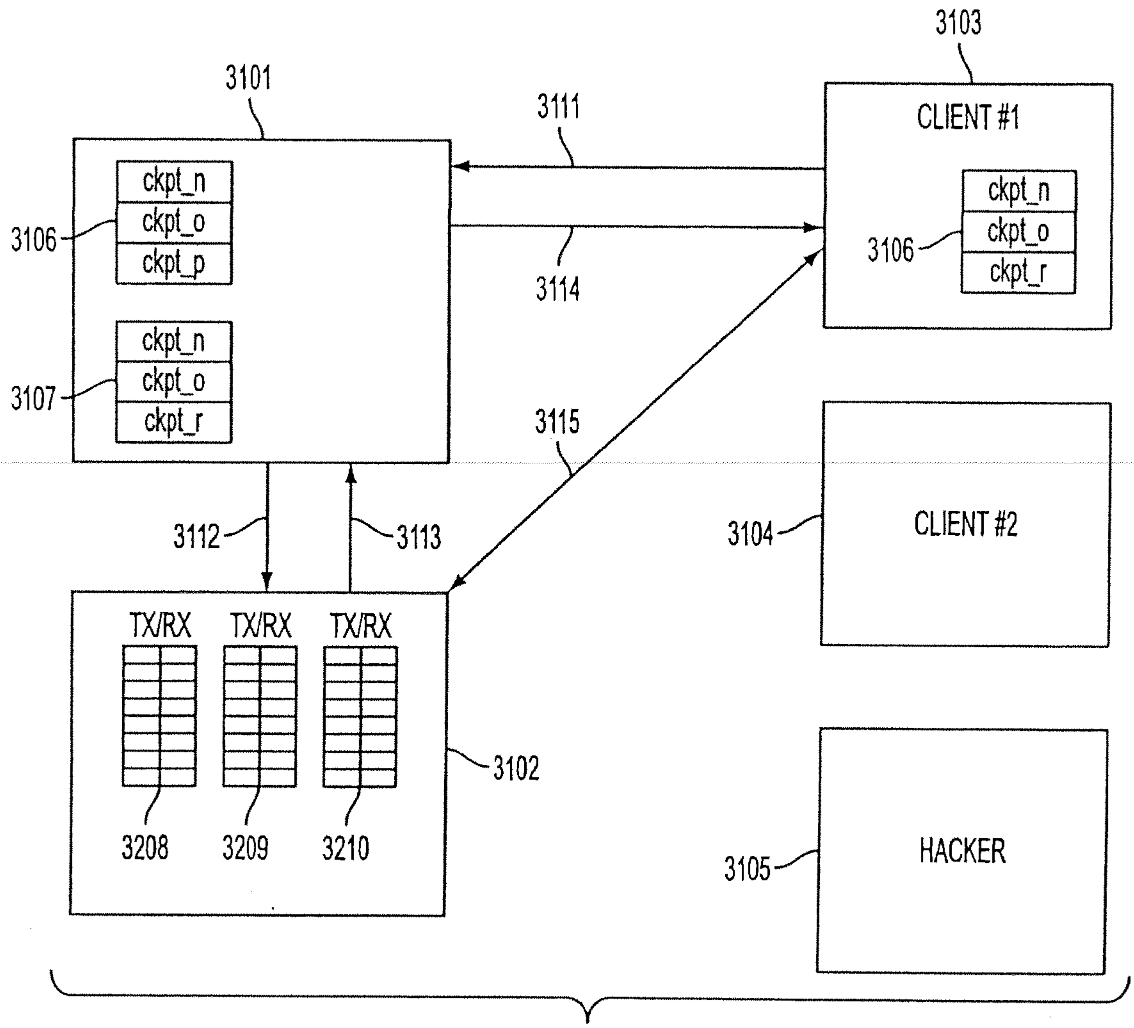

3103
3101
3111
CLIENT #1
ckpt_n
ckpt_o
ckpt_p
3106
ckpt_n
ckpt_o
ckpt_r
3106
3114
ckpt_n
ckpt_o
ckpt_r
3107
3115
3112
3113
3104
CLIENT #2
TX/RX
TX/RX
TX/RX
3102
3208
3209
3210
3105
HACKER

FIG. 31

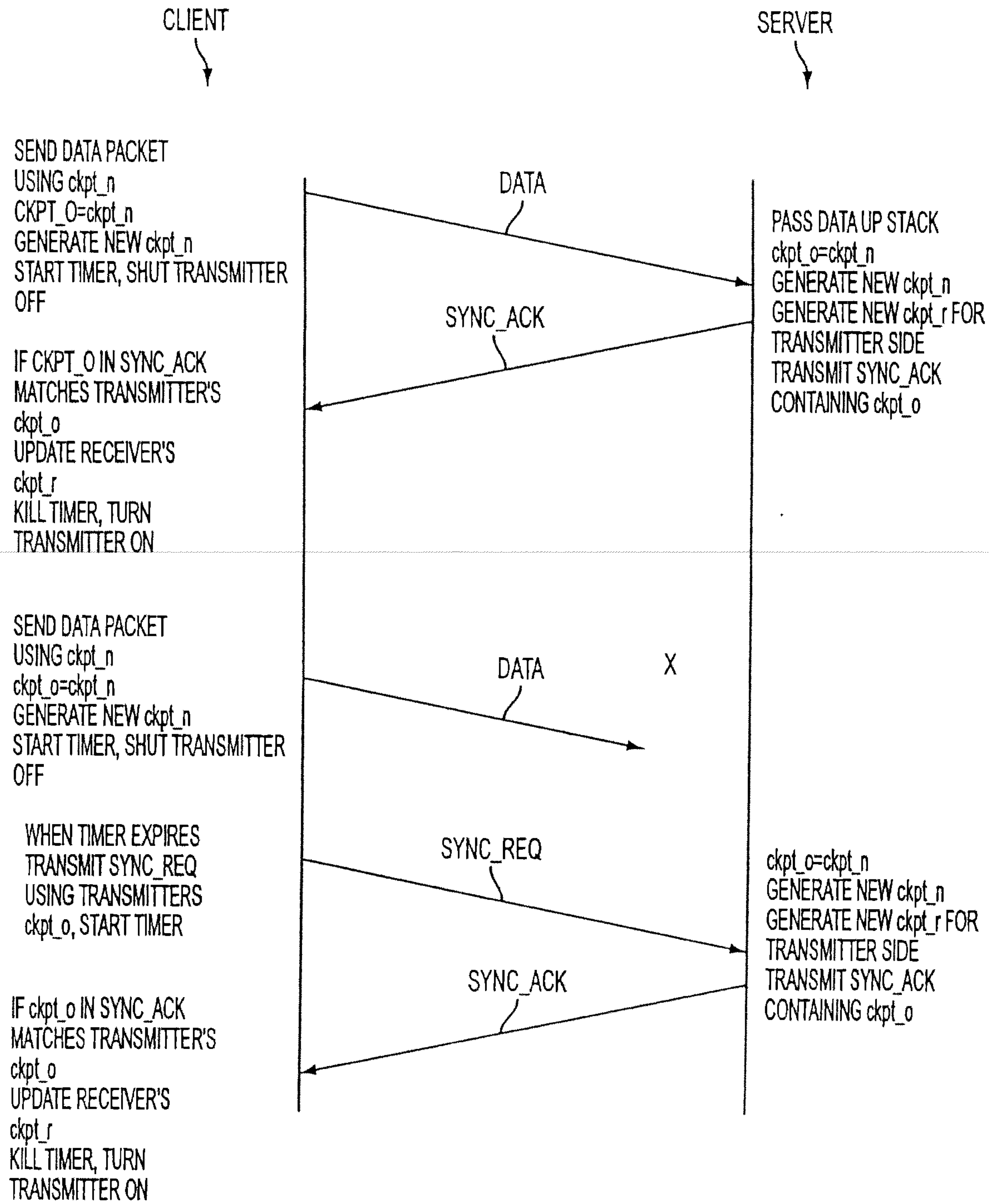

CLIENT
SERVER
SEND DATA PACKET
USING ckpt_n
CKPT_O=ckpt_n
GENERATE NEW ckpt_n
START TIMER, SHUT TRANSMITTER
OFF
DATA
PASS DATA UP STACK
ckpt_o=ckpt_n
GENERATE NEW ckpt_n
GENERATE NEW ckpt_r FOR
TRANSMITTER SIDE
TRANSMIT SYNC_ACK
CONTAINING ckpt_o
SYNC_ACK
IF CKPT_O IN SYNC_ACK
MATCHES TRANSMITTER'S
ckpt_o
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

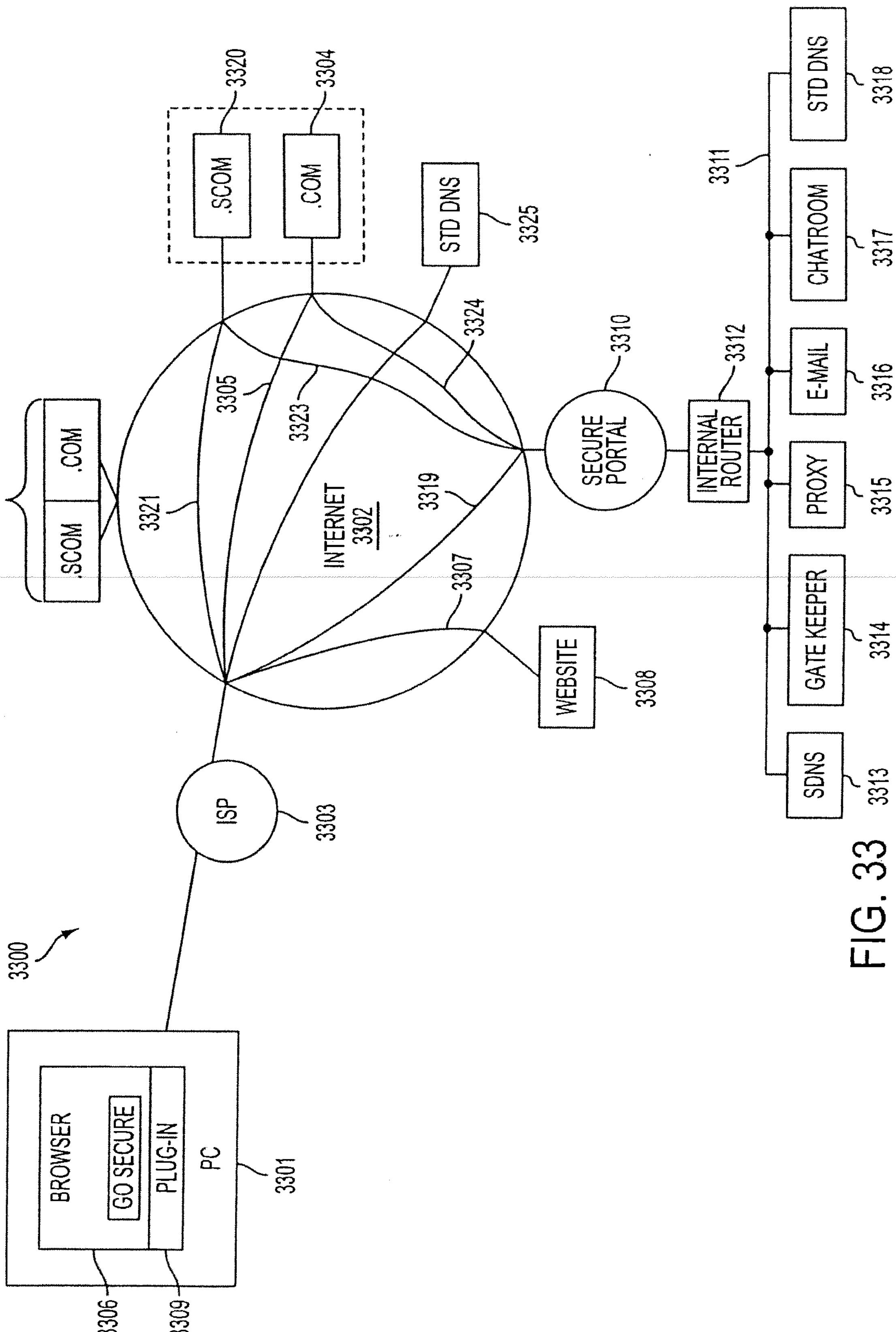

3300
BROWSER
GO SECURE
PLUG-IN
PC
3301
3306
3309
ISP
3303
3322
.SCOM
.COM
.SCOM
3320
.COM
3304
STD DNS
3325
INTERNET
3302
3321
3305
3323
3324
3319
3307
WEBSITE
3308
SECURE PORTAL
3310
INTERNAL ROUTER
3312
3311
SDNS
3313
GATE KEEPER
3314
PROXY
3315
E-MAIL
3316
CHATROOM
3317
STD DNS
3318

FIG. 33

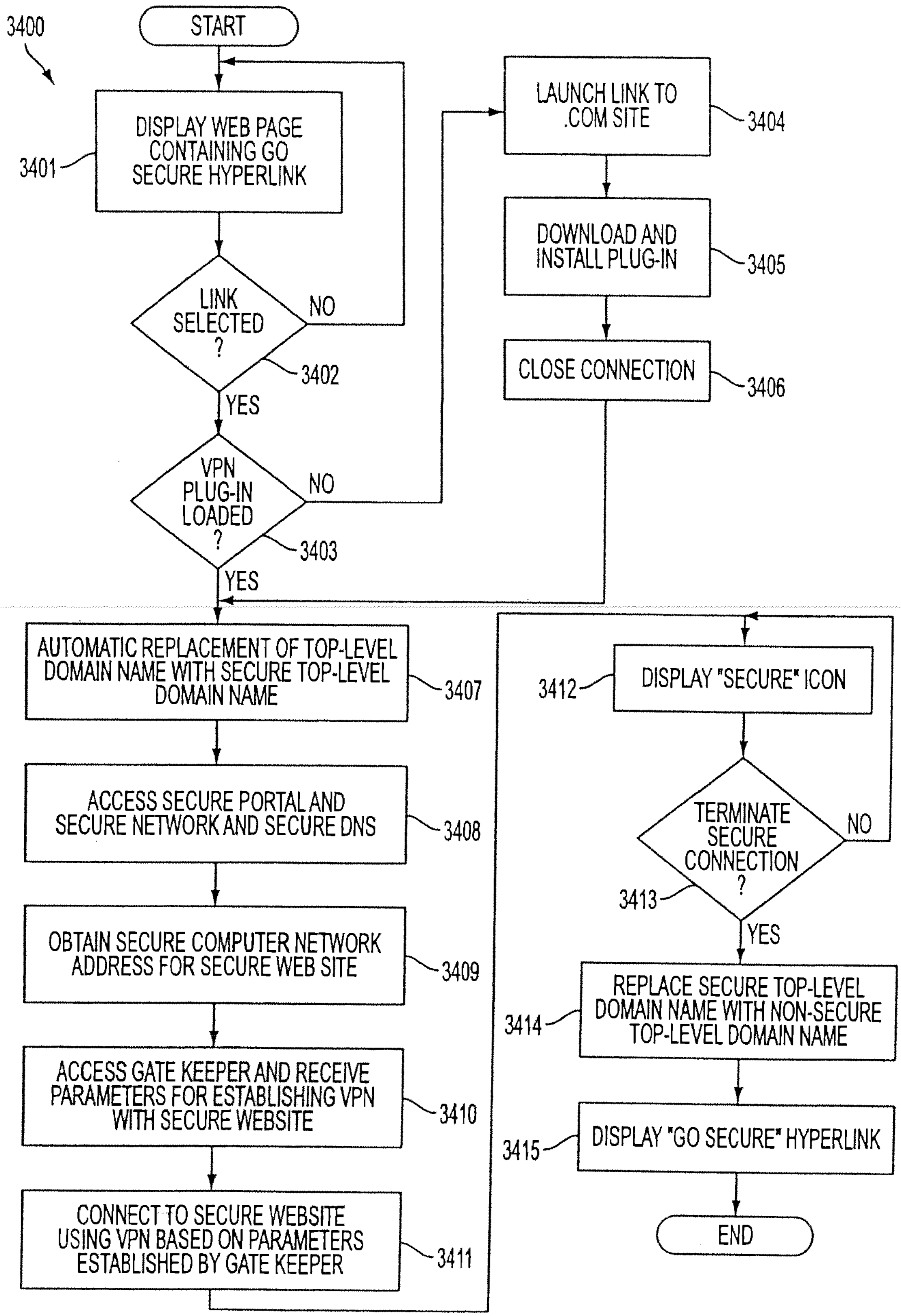

3400
START
DISPLAY WEB PAGE CONTAINING GO SECURE HYPERLINK
3401
LINK SELECTED ?
NO
3402
YES
VPN PLUG-IN LOADED ?
NO
3403
YES
LAUNCH LINK TO .COM SITE
3404
DOWNLOAD AND INSTALL PLUG-IN
3405
CLOSE CONNECTION
3406
AUTOMATIC REPLACEMENT OF TOP-LEVEL DOMAIN NAME WITH SECURE TOP-LEVEL DOMAIN NAME
3407
ACCESS 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
3415
DISPLAY "GO SECURE" HYPERLINK
END

FIG. 34

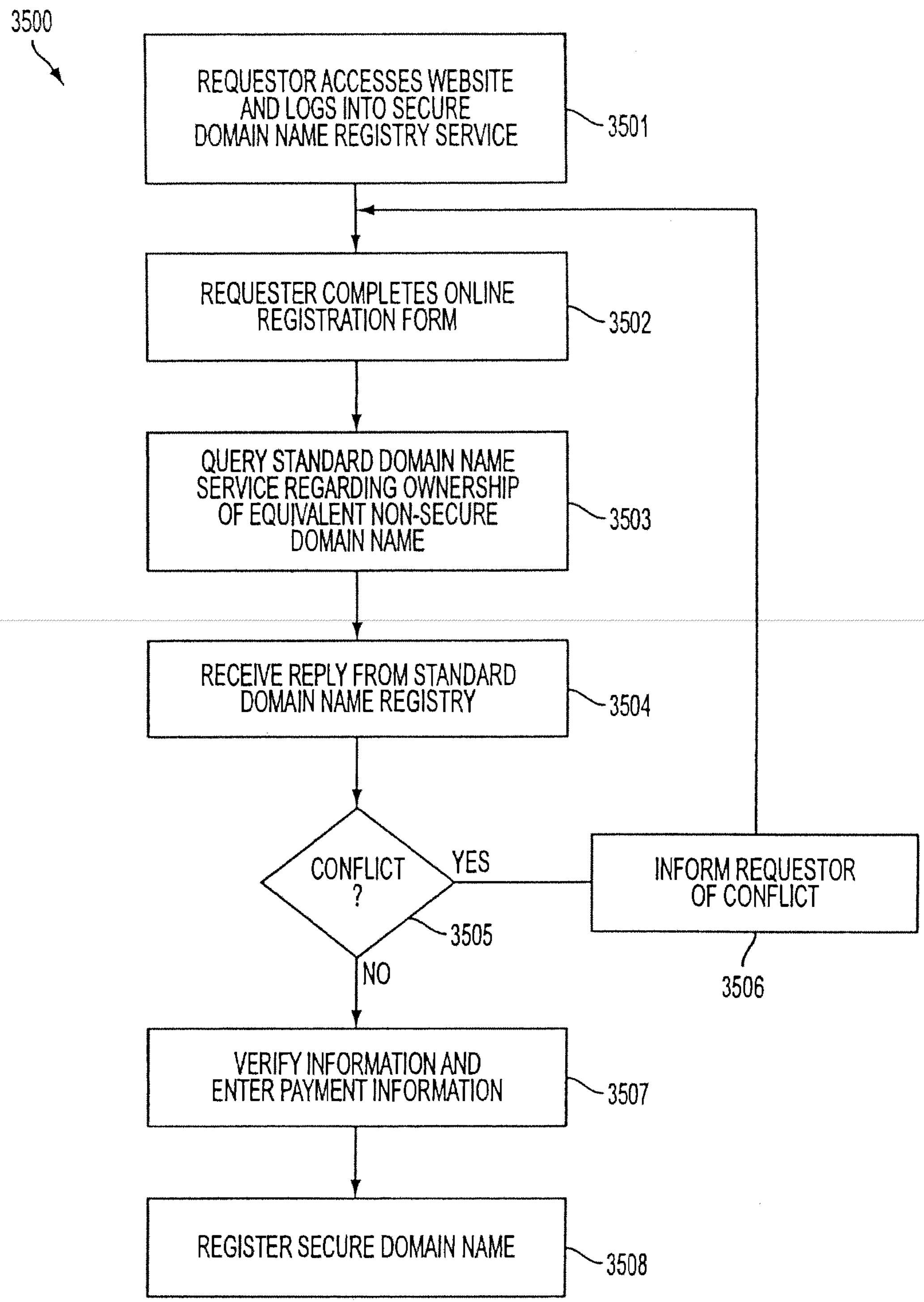

3500
REQUESTOR ACCESSES WEBSITE AND LOGS INTO SECURE DOMAIN NAME REGISTRY SERVICE
3501
REQUESTER COMPLETES ONLINE REGISTRATION FORM
3502
QUERY STANDARD DOMAIN NAME SERVICE REGARDING OWNERSHIP OF EQUIVALENT NON-SECURE DOMAIN NAME
3503
RECEIVE REPLY FROM STANDARD DOMAIN NAME REGISTRY
3504
CONFLICT ?
YES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

FIG. 35

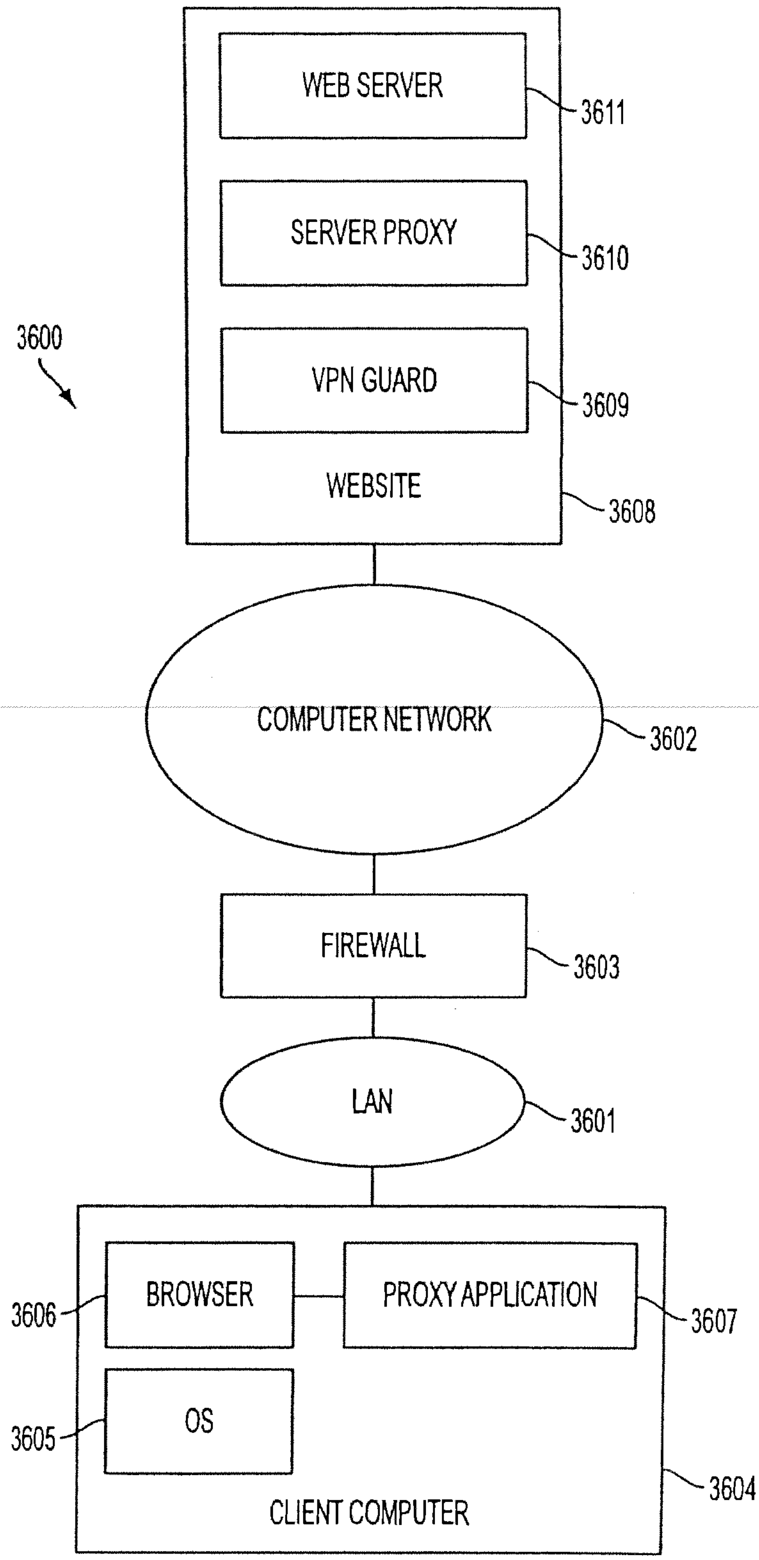

WEB SERVER
3611
SERVER PROXY
3610
3600
VPN GUARD
3609
WEBSITE
3608
COMPUTER NETWORK
3602
FIREWALL
3603
LAN
3601
BROWSER
PROXY APPLICATION
3606
3607
OS
3605
3604
CLIENT COMPUTER

FIG. 36

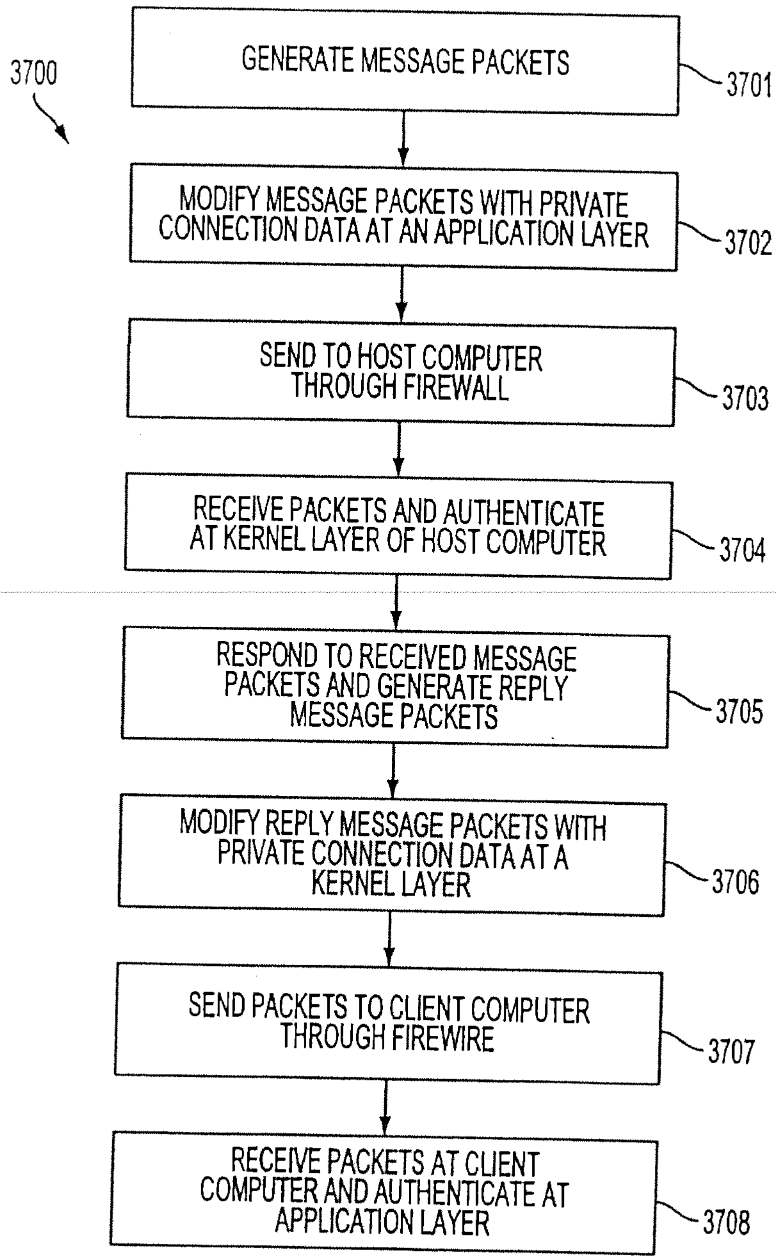

3700
GENERATE MESSAGE PACKETS
3701
MODIFY MESSAGE PACKETS WITH PRIVATE CONNECTION DATA AT AN APPLICATION LAYER
3702
SEND TO HOST COMPUTER THROUGH FIREWALL
3703
RECEIVE PACKETS AND AUTHENTICATE AT KERNEL LAYER OF HOST COMPUTER
3704
RESPOND TO RECEIVED MESSAGE PACKETS AND GENERATE REPLY MESSAGE PACKETS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

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor LARSON
Filer:	Toby H. Kusmer./Kimila Carraway
Attorney Docket Number:	077580-0177

Filed as Large Entity

Utility 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
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1250**

Electronic Acknowledgement Receipt

EFS ID:	13742625
Application Number:	13615557
International Application Number:	
Confirmation Number:	1089
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor LARSON
Customer Number:	23630
Filer:	Toby H. Kusmer./Kimila Carraway
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	077580-0177
Receipt Date:	13-SEP-2012
Filing Date:	
Time Stamp:	23:27:46
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1250
RAM confirmation Number	8918
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		077580-0177_Continuation_Application.pdf	1703386 bd95cc617981435b1b18687ff4fa2ceb0ff2fe59	yes	143

Multipart Description/PDF files in .zip description

Document Description	Start	End
Application Data Sheet	1	5
Oath or Declaration filed	6	11
Specification	12	99
Claims	100	102
Abstract	103	103
Drawings-only black and white line drawings	104	143

Warnings:

Information:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
2	Fee Worksheet (SB06)	fee-info.pdf	33236 7e406a30389737976bb02fd59c248f8eac08e954	no	2

Warnings:

Information:

Total Files Size (in bytes): 1736622

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 Data Sheet 37 CFR 1.76	Attorney Docket Number	077580-0177
	Application Number	

Title of Invention	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

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	US

Citizenship under 37 CFR 1.41(b)	US

Mailing Address of Applicant:

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

Applicant 2

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	US

Citizenship under 37 CFR 1.41(b)	US

Mailing Address of Applicant:

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

Applicant 3

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
	Edmund	Colby	MUNGER	

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

City	Crownsville	State/Province	MD	Country of Residence	US

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	077580-0177
	Application Number	

Title of Invention	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

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

Applicant 4

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**	US
Citizenship under 37 CFR 1.41(b)	US				

Mailing Address of Applicant:			
Address 1	26203 Ocala Circle		
Address 2			
City	South Riding	**State/Province**	VA
Postal Code	20152	**Country**	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		Add Email Remove Email

Application Information:

Title of the Invention	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES		
Attorney Docket Number	077580-0177	**Small Entity Status Claimed**	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		**Sub Class (if any)**	
Suggested Technology Center (if any)	2453		
Total Number of Drawing Sheets (if any)	40	**Suggested Figure for Publication (if any)**	

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	077580-0177
	Application Number	

Title of Invention	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	13049552	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)
13049552	Continuation of	11840560	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)
11840560	Continuation of	10714849	2003-11-18	7418504	2008-08-26

Prior Application Status	Abandoned		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
10714849	Continuation of	09558210	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)
09558210	Continuation in part of	09504783	2000-02-15	6502135	2002-12-31

Prior Application Status	Patented		Remove

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	077580-0177
	Application Number	

Title of Invention	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)
09504783	Continuation in part of	09429643	1999-10-29	7010604	2006-03-07

Prior Application Status	Expired		Remove
Application Number	**Continuity Type**	**Prior Application Number**	**Filing Date (YYYY-MM-DD)**
09429643	non provisional of	60137704	1999-06-07
Prior Application Status	Expired		Remove
Application Number	**Continuity Type**	**Prior Application Number**	**Filing Date (YYYY-MM-DD)**
09429643	non provisional of	60106261	1998-10-30

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

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.

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

If the Assignee is an Organization check here. ☒

Organization Name	VIRNETX, INC.

Mailing Address Information:

Address 1	P.O. Box 439		
Address 2			
City	Zephyr Cove	**State/Province**	NV
Country[i]	US	Postal Code	89448
Phone Number		Fax Number	
Email Address			

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

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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	077580-0177
	Application Number	

Title of Invention	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

Signature	/Toby H. Kusmar/			Date (YYYY-MM-DD)	2012-09-13
First Name	Toby H.	Last Name	Kusmar	Registration Number	26418

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
13/615,557	09/13/2012	Victor Larson	077580-0177

CONFIRMATION NO. 1089

FORMALITIES LETTER

OC000000056885489

23630
McDermott Will & Emery
The McDermott Building
500 North Capitol Street, N.W.
Washington, DC 20001

Date Mailed: 10/04/2012

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:

- Replacement drawings in compliance with 37 CFR 1.84 and 37 CFR 1.121(d) are required. The drawings submitted are not acceptable because:
  - The drawings must be reasonably free from erasures and must be free from alterations, overwriting, interlineations, folds, and copy marks. See Figure(s) all.
- 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.

/ebanaybanay/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/615,557

APPLICATION AS FILED - PART I

FOR	NUMBER FILED (Column 1)	NUMBER EXTRA (Column 2)	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))	20 minus 20 =	*			OR	x 60 =	0.00
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
			TOTAL			TOTAL	1250

* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED - PART II

AMENDMENT A

	CLAIMS REMAINING AFTER AMENDMENT (Column 1)		HIGHEST NUMBER PREVIOUSLY PAID FOR (Column 2)	PRESENT EXTRA (Column 3)	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))	*	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	

AMENDMENT B

	CLAIMS REMAINING AFTER AMENDMENT (Column 1)		HIGHEST NUMBER PREVIOUSLY PAID FOR (Column 2)	PRESENT EXTRA (Column 3)	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 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
13/615,557	09/13/2012	2431	1250	077580-0177	20	2

CONFIRMATION NO. 1089

23630
McDermott Will & Emery
The McDermott Building
500 North Capitol Street, N.W.
Washington, DC 20001

FILING RECEIPT

OC000000056885488

Date Mailed: 10/04/2012

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**

Inventor(s)

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

Applicant(s)

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

Assignment For Published Patent Application

VIRNETX, INC., Zephyr Cove, NV

Power of Attorney: The patent practitioners associated with Customer Number 22907

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: 10/02/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/615,557**

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

Non-Publication Request: No

Early Publication Request: No

Title

AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

Preliminary Class

713

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).

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).

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Dates	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication/Patent Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1	09/399,753	09/22/1998	Graig Miller et al.	
	A2	60/151,563	08/31/1999	Bryan Whittles	
	A3	60/134,547	05/17/1999	Victory Sheymov	
	A4	2,895,502	07/21/1959	Roper et al.	
	A5	4,761,334	08/1988	Sagoi et al.	
	A6	4,885,778	12/5/1989	Weiss, Kenneth	
	A7	4,920,484	4/24/1990	Ranade	
	A8	4,933,846	06/12/1990	Humphrey et al.	
	A9	4,952,930	08/28/1990	Franaszek et al.	
	A10	4,988,990	01/29/1991	Warrior	
	A11	5,164,988	11/17/1992	Matyas	
	A12	5,204,961	04/20/1993	Barlow	
	A13	5,276,735	01/04/1994	Boebert et al	
	A14	5,303,302	04/12/1994	Burrows	
	A15	5,311,593	05/10/1994	Carmi	
	A16	5,329,521	07/12/1994	Walsh et al.	
	A17	5,341,426	08/23/1994	Barney et al.	
	A18	5,367,643	11/22/1994	Chang et al	
	A19	5,384,848	01/24/1995	Kikuchi	
	A20	5,511,122	04/23/1996	Atkinson	
	A21	5,548,646	08/20/1996	Aziz et al.	
	A22	5,559,883	09/24/1996	Williams	
	A23	5,561,669	10/01/1996	Lenney et al	
	A24	5,588,060	12/24/1996	Aziz	
	A25	5,590,285	12/31/1996	Krause et al.	
	A26	5,625,626	04/29/1997	Umekita	
	A27	5,629,984	05/13/1997	McManis	
	A28	5,654,695	08/05/1997	Olnowich et al	
	A29	5,682,480	10/28/1997	Nakagawa	
	A30	5,689,566	11/18/1997	Nguyen	
	A31	5,689,641	11/18/1997	Ludwig et al.	
	A32	5,740,375	04/14/1998	Dunne et al.	
	A33	5,757,925	05/1998	Faybishenko	
	A34	5,764,906	06/1998	Edelstein et al.	
	A35	5,771,239	06/23/1998	Moroney et al.	
	A36	5,774,660	6/30/1998	Brendel et al	
	A37	5,787,172	07/28/1998	Arnold	
	A38	5,790,548	08/04/1998	Sitaraman et al.	
	A39	5,796,942	08/18/1998	Esbensen	
	A40	5,805,801	09/08/1998	Holloway et al.	
	A41	5,805,803	09/08/1998	Birrell et al.	
	A42	5,822,434	10/13/1998	Caronni et al.	
	A43	5,842,040	11/24/1998	Hughes et al.	
	A44	5,845,091	12/01/1998	Dunne et al.	
	A45	5,864,666	01/1999	Shrader, Theodore Jack London	
	A46	5,867,650	02/02/1998	Osterman	
	A47	5,870,610	02/09/1999	Beyda et al.	
	A48	5,878,231	05/02/1999	Baehr et al	
	A49	5,892,903	04/06/1999	Klaus	
	A50	5,898,830	04/27/1999	Wesinger, Jr. et al.	
	A51	5,905,859	05/18/1999	Holloway et al.	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Dates	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication/Patent Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A52	5,918,018	06/29/1999	Gooderum et al.	
	A53	5,918,019	06/29/1999	Valencia	
	A54	5,950,195	09/07/1999	Stockwell et al.	
	A55	5,950,519	09/14/1999	Anatoli	
	A56	5,960,204	09/28/1999	Yinger et al.	
	A57	5,996,016	11/30/1999	Thalheimer et al.	
	A58	6,006,259	12/21/1999	Adelman et al.	
	A59	6,006,272	12/21/1999	Aravamudan et al	
	A60	6,016,318	01/18/2000	Tomoike	
	A61	6,016,512	01/18/2000	Huitema	
	A62	6,041,342	03/21/2000	Yamaguchi	
	A63	6,052,788	04/2000	Wesinger et al.	
	A64	6,055,574	04/25/2000	Smorodinsky et al.	
	A65	6,061,346	05/2000	Nordman, Mikael	
	A66	6,061,736	05/09/2000	Rochberger et al	
	A67	6,079,020	06/20/2000	Liu	
	A68	6,081,900	06/2000	Subramaniam et al.	
	A69	6,092,200	07/18/2000	Muniyappa et al.	
	A70	6,101,182	08/2000	Sistanizadeh et al.	
	A71	6,119,171	09/12/2000	Alkhatib	
	A72	6,119,234	09/12/2000	Aziz et al.	
	A73	6,131,121	10/10/2000	Mattaway et al.	
	A74	6,147,976	11/14/2000	Shand et al.	
	A75	6,157,957	12/05/2000	Berthaud	
	A76	6,158,011	12/05/2000	Chen et al.	
	A77	6,168,409	01/02/2001	Fare	
	A78	6,173,399	01/09/2001	Gilbrech	
	A79	6,175,867	01/16/2001	Taghadoss	
	A80	6,178,409	01/23/2001	Weber et al.	
	A81	6,178,505	01/23/2001	Schneider et al	
	A82	6,179,102	01/30/2001	Weber, et al.	
	A83	6,182,141	1/30/2001	Blum et al.	
	A84	6,199,112	03/2001	Wilson, Stephen K.	
	A85	6,202,081	03/2001	Naudus, Stanley T.	
	A86	6,222,842	04/24/2001	Sasyan et al.	
	A87	6,223,287	04/24/2001	Douglas et al.	
	A88	6,226,748	05/01/2001	Bots et al.	
	A89	6,226,751	05/01/2001	Arrow et al..	
	A90	6,233,618	05/15/2001	Shannon	
	A91	6,243,360	06/05/2001	Basilico	
	A92	6,243,749	06/05/2001	Sitaraman et al.	
	A93	6,243,754	06/05/2001	Guerin et al	
	A94	6,246,670	06/12/2001	Karlsson et al.	
	A95	6,256,671	07/03/2001	Strentzsch et al.	
	A96	6,262,987	07/17/01	Mogul, Jeffrey C.	
	A97	6,263,445	07/17/2001	Blumenau	
	A98	6,269,099	07/31/2001	Borella et al.	
	A99	6,286,047	09/04/2001	Ramanathan et al	
	A100	6,298,341	10/02/01	Mann, et al.	
	A101	6,301,223	10/9/2001	Hrastar et al	
	A102	6,308,213	10/23/2001	Valencia	
	A103	6,308,274	10/23/2001	Swift	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Dates	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication/Patent Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A104	6,311,207	10/30/2001	Mighdoll et al	
	A105	6,314,463	11/2001	Abbott et al.	
	A106	6,324,161	11/27/2001	Kirch	
	A107	6,330,562	12/11/2001	Boden et al.	
	A108	6,332,158	12/18/2001	Risley et al.	
	A109	6,333,272	12/25/01	McMillin, et al.	
	A110	6,338,082	01/08/02	Schneider, Eric	
	A111	6,353,614	03/05/2002	Borella et al.	
	A112	6,425,003	07/23/2002	Herzog et al.	
	A113	6,430,155	08/06/2002	Davie et al	
	A114	6,430,610	08/06/2002	Carter	
	A115	6,487,598	11/26/2002	Valencia	
	A116	6,496,867	12/17/2002	Beser et al.	
	A117	6,499,108	12/24/2002	Johnson	
	A118	6,502,135	12/2002	Munger et al.	
	A119	6,505,232	01/07/2003	Mighdoll et al	
	A120	6,510,154	01/21/2003	Mayes et al	
	A121	6,549,516	04/15/2003	Albert et al	
	A122	6,557,037	04/2003	Provino, Joseph E.	
	A123	6,560,634	05/06/2003	Broadhurst	
	A124	6,571,296	05/27/2002	Dillon	
	A125	6,571,338	05/27/2003	Shaio et al.	
	A126	6,581,166	7/17/2003	Hirst et al.	
	A127	6,606,708	08/12/2003	Devine et al.	
	A128	6,615,357	9/2/2003	Boden et al.	
	A129	6,618,761	09/09/2003	Munger et al.	
	A130	6,671,702	12/30/2003	Kruglikov et al	
	A131	6,687,551	2/3/2004	Steindl	
	A132	6,687,746	02/03/04	Shuster, et al.	
	A133	6,701,437	03/02/2004	Hoke et al.	
	A134	6,714,970	3/30/2004	Fiveash et al.	
	A135	6,717,949	4/6/2004	Boden et al.	
	A136	6,751,738	06/15/2004	Wesinger, Jr. et al..	
	A137	6,752,166	06/22/04	Lull, et al.	
	A138	6,757,740	06/29/04	Parekh, et al.	
	A139	6,760,766	7/6/2004	Sahlqvist	
	A140	6,813,777	11/2004	Weinberger et al.	
	A141	6,826,616	11/30/2004	Larson et al.	
	A142	6,839,759	1/4/2005	Larson et al.	
	A143	6,937,597	08/30/2005	Rosenberg et al.	
	A144	7,010,604	3/7/2006	Munger et al.	
	A145	7,039,713	05/2006	Van Gunter et al.	
	A146	7,072,964	07/04/2006	Whittle et al.	
	A147	7,133,930	11/7/2006	Munger et al.	
	A148	7,167,904	01/23/07	Devarajan, et al.	
	A149	7,188,175	03/06/07	McKeeth, James A.	
	A150	7,188,180	3/6/2007	Larson et al.	
	A151	7,197,563	3/27/2007	Sheymov et al.	
	A152	7,353,841	04/08/08	Kono, et al.	
	A153	7,418,504	08/2008	Larson et al.	
	A154	7,461,334	12/02/08	Lu, et al.	
	A155	7,490,151	02/2009	Munger et al.	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Dates	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication/Patent Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A156	7,493,403	02/2009	Shull et al.	
	A157	7,584,500	09/2009	Dillon et al.	
	A158	7,764,231	07/27/2010	Karr et al.	
	A159	7,852,861	12/2010	Wu et al.	
	A160	7,921,211	04/2011	Larson et al.	
	A161	7,933,990	04/2011	Munger et al.	
	A162	8,051,181	11/2011	Larson et al.	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

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.	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

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	Translation 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			
	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			

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

		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.	
	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.	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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	I. 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)	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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)	
	D52	Aventail Corp., "Managing Corporate Access to the Internet," Aventail AutoSOCKS White Paper *available at* http://web.archive.org/19970620030312/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)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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)	
	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, Intemet 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)	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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)	
	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)	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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)	
	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)	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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)	
	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	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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)	
	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)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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)	
	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)	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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)	
	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," 9 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)	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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	
	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 Intemet 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)	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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	
	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 vs. Claims of the '211 Patent	
	D316	Exhibit 2, IETF RFC 2065: Domain Name System Security Extensions; Published January 1997 vs. Claims of the '504 Patent	
	D317	Exhibit 3, RFC 2543 vs. Claims of the '135 Patent	
	D318	Exhibit 4, RFC 2543 vs. Claims of the '211 Patent	
	D319	Exhibit 5, RFC 2543 vs. Claims of the '504 Patent	
	D320	Exhibit 6, SIP Draft v.2 vs. Claims of the '135 Patent	
	D321	Exhibit 7, SIP Draft v.2 vs. Claims of the '211 Patent	
	D322	Exhibit 8, SIP Draft v.2 vs. Claims of the '504 Patent	
	D323	Exhibit 9, H.323 vs. Claims of the '135 Patent	
	D324	Exhibit 10, H.323 vs. Claims of the '211 Patent	
	D325	Exhibit 11, H.323 vs. Claims of the '504 Patent	
	D326	Exhibit 12, SSL 3.0 vs. Claims of the '135 Patent .	
	D327	Exhibit 13, SSL 3.0 vs. Claims of the '211 Patent	
	D328	Exhibit 14, SSL 3.0 vs. Claims of the '504 Patent	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D329	Exhibit 15, RFC 2487 vs. Claims of the '135 Patent	
	D330	Exhibit 16, RFC 2487 vs. Claims of the '211 Patent	
	D331	Exhibit 17, RFC 2487 vs. Claims of the '504 Patent	
	D332	Exhibit 18, RFC 2595 vs. Claims of the '135 Patent	
	D333	Exhibit 19, RFC 2595 vs. Claims of the '211 Patent	
	D334	Exhibit 20, RFC 2595 vs. Claims of the '504 Patent	
	D335	Exhibit 21, iPass vs. Claims of the '135 Patent	
	D336	Exhibit 22, iPASS vs. Claims of the '211 Patent	
	D337	Exhibit 23, iPASS vs. Claims of the '504 Patent	
	D338	Exhibit 24, "US '034" vs. Claims of the '135 Patent	
	D339	Exhibit 25, US Patent No. 6,453,034 ("US '034") vs. Claims of the '211 Patent	
	D340	Exhibit 26, US Patent No. 6,453,034 ("US '034") vs. Claims of the '504 Patent	
	D341	Exhibit 27, US '287 vs. Claims of the '135 Patent	
	D342	Exhibit 28, US '287 vs. Claims of the '211 Patent	
	D343	Exhibit 29, US '287 vs. Claims of the '504 Patent	
	D344	Exhibit 30, Overview of Access VPNs vs. Claims of the '135 Patent	
	D345	Exhibit 31, Overview of Access VPNs vs. Claims of the '211 Patent	
	D346	Exhibit 32, Overview of Access VPNs vs. Claims of the '504 Patent	
	D347	Exhibit 34, RFC 1928 vs. Claims of the '135 Patent	
	D348	Exhibit 35, RFC 1928 vs. Claims of the '211 Patent	
	D349	Exhibit 36, RFC 1928 vs. Claims of the '504 Patent	
	D350	Exhibit 37, RFC 2661 vs. Claims of the '135 Patent	
	D351	Exhibit 38, RFC 2661 vs. Claims of the '211 Patent	
	D352	Exhibit 39, RFC 2661 vs. Claims of the '504 Patent	
	D353	Exhibit 40, SecureConnect vs. Claims of the '135 Patent	
	D354	Exhibit 41, SecureConnect vs. Claims of the '211 Patent	
	D355	Exhibit 42,SecureConnect vs. Claims of the '504 Patent	
	D356	Exhibit 43, SFS-HTTP vs. Claims of the '135 Patent	
	D357	Exhibit 44, SFS-HTTP vs. Claims of the '211 Patent	
	D358	Exhibit 45, SFS-HTTP vs. Claims of the '504 Patent	
	D359	Exhibit 46, US '883 vs. Claims of the '135 Patent	
	D360	Exhibit 47, US '883 vs. Claims of the '211 Patent	
	D361	Exhibit 48, US '883 vs. Claims of the '504 Patent	
	D362	Exhibit 49, US '132 vs. Claims of the '135 Patent	
	D363	Exhibit 50, US '132 vs. Claims of the '211 Patent	
	D364	Exhibit 51, US '132 vs. Claims of the '504 Patent	
	D365	Exhibit 52, US '213 vs. Claims of the '135 Patent	
	D366	Exhibit 53, US '213 vs. Claims of the '211 Patent	
	D367	Exhibit 54, US '213 vs. Claims of the '504 Patent	
	D368	Exhibit 55, B&M VPNs vs. Claims of the '135 Patent	
	D369	Exhibit 56, B&M VPNs vs. Claims of the '211 Patent	
	D370	Exhibit 57, B&M VPNs vs. Claims of the '504 Patent	
	D371	Exhibit 58, BorderManager vs. Claims of the '135 Patent	
	D372	Exhibit 59, BorderManager vs. Claims of the '211 Patent	
	D373	Exhibit 60, BorderManager vs. Claims of the '504 Patent	
	D374	Exhibit 61, Prestige 128 Plus vs. Claims of the '135 Patent	
	D375	Exhibit 62, Prestige 128 Plus vs. Claims of the '211 Patent	
	D376	Exhibit 63, Prestige 128 Plus vs. Claims of the '504 Patent	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D377	Exhibit 64, RFC 2401 vs. Claims of the '135 Patent	
	D378	Exhibit 65, RFC 2401 vs. Claims of the '211 Patent	
	D379	Exhibit 66, RFC 2401 vs. Claims of the '504 Patent	
	D380	Exhibit 67, RFC 2486 vs. Claims of the '135 Patent	
	D381	Exhibit 68, RFC 2486 vs. Claims of the '211 Patent	
	D382	Exhibit 69, RFC 2486 vs. Claims of the '504 Patent	
	D383	Exhibit 70, Understanding IPSec vs. Claims of the '135 Patent	
	D384	Exhibit 71, Understanding IPSec vs. Claims of the '211 Patent	
	D385	Exhibit 72, Understanding IPSec vs. Claims of the '504 Patent	
	D386	Exhibit 73, US '820 vs. Claims of the '135 Patent	
	D387	Exhibit 74, US '820 vs. Claims of the '211 Patent	
	D388	Exhibit 75, US '820 vs. Claims of the '504 Patent	
	D389	Exhibit 76, US '019 vs. Claims of the '211 Patent	
	D390	Exhibit 77, US '019 vs. Claims of the '504 Patent	
	D391	Exhibit 78, US '049 vs. Claims of the '135 Patent	
	D392	Exhibit 79, US '049 vs. Claims of the '211 Patent	
	D393	Exhibit 80, US '049 vs. Claims of the '504 Patent	
	D394	Exhibit 81, US '748 vs. Claims of the '135 Patent	
	D395	Exhibit 82, US '261 vs. Claims of the '135 Patent	
	D396	Exhibit 83, US '261 vs. Claims of the '211 Patent	
	D397	Exhibit 84, US '261 vs. Claims of the '504 Patent	
	D398	Exhibit 85, US '900 vs. Claims of the '135 Patent	
	D399	Exhibit 86, US '900 vs. Claims of the '211 Patent	
	D400	Exhibit 87, US '900 vs. Claims of the '504 Patent	
	D401	Exhibit 88, US '671 vs. Claims of the '135 Patent	
	D402	Exhibit 89, US '671 vs. Claims of the '211 Patent	
	D403	Exhibit 90, US '671 vs. Claims of the '504 Patent	
	D404	Exhibit 91, JP '704 vs. Claims of the '135 Patent	
	D405	Exhibit 92, JP '704 vs. Claims of the '211 Patent	
	D406	Exhibit 93, JP '704 vs. Claims of the '504 Patent	
	D407	Exhibit 94, GB '841 vs. Claims of the '135 Patent	
	D408	Exhibit 95, GB '841 vs. Claims of the '211 Patent	
	D409	Exhibit 96, GB '841 vs. Claims of the '504 Patent	
	D410	Exhibit 97, US '318 vs. Claims of the '135 Patent	
	D411	Exhibit 98, US '318 vs. Claims of the '211 Patent	
	D412	Exhibit 99, US '318 vs. Claims of the '504 Patent	
	D413	Exhibit 100, VPN/VLAN vs. Claims of the '135 Patent	
	D414	Exhibit 101, Nikkei vs. Claims of the '135 Patent	
	D415	Exhibit 102, NIKKEI vs. Claims of the '211 Patent	
	D416	Exhibit 103, NIKKEI vs. Claims of the '504 Patent	
	D417	Exhibit 104, Special Anthology vs. Claims of the '135 Patent	
	D418	Exhibit 105, Omron vs. Claims of the '135 Patent	
	D419	Exhibit 106, Gauntlet System vs. Claims of the '135 Patent	
	D420	Exhibit 107, Gauntlet System vs. Claims of the '151 Patent	
	D421	Exhibit 108, Gauntlet System vs. Claims of the '180 Patent	
	D422	Exhibit 109, Gauntlet System vs. Claims of the '211 Patent	
	D423	Exhibit 110, Gauntlet System vs. Claims of the '504 Patent	
	D424	Exhibit 111, Gauntlet System vs. Claims of the '759 Patent	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D425	Exhibit 112, IntraPort System vs. Claims of the '135 Patent	
	D426	Exhibit 113, IntraPort System vs. Claims of the '151 Patent	
	D427	Exhibit 114, IntraPort System vs. Claims of the '180 Patent	
	D428	Exhibit 115, IntraPort System vs. Claims of the '211 Patent	
	D429	Exhibit 116, IntraPort System vs. Claims of the '504 Patent	
	D430	Exhibit 117, IntraPort System vs. Claims of the '759 Patent	
	D431	Exhibit 118, Altiga VPN System vs. Claims of the '135 Patent	
	D432	Exhibit 119, Altiga VPN System vs. Claims of the '151 Patent	
	D433	Exhibit 120, Altiga VPN System vs. Claims of the '180 Patent	
	D434	Exhibit 121, Altiga VPN System vs. Claims of the '211 Patent	
	D435	Exhibit 122, Altiga VPN System vs. Claims of the '504 Patent	
	D436	Exhibit 123, Altiga VPN System vs. Claims of the '759 Patent	
	D437	Exhibit 124, Kiuchi vs. Claims of the '135 Patent	
	D438	Exhibit 125, Kiuchi vs. Claims of the '151 Patent	
	D439	Exhibit 126, Kiuchi vs. Claims of the '180 Patent	
	D440	Exhibit 127, Kiuchi vs. Claims of the '211 Patent	
	D441	Exhibit 128, Kiuchi vs. Claims of the '504 Patent	
	D442	Exhibit 129, Kiuchi vs. Claims of the '759 Patent	
	D443	Exhibit 130, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '135 Patent	
	D444	Exhibit 131, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '151 Patent	
	D445	Exhibit 132, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '180 Patent	
	D446	Exhibit 133, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '211 Patent	
	D447	Exhibit 134, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '504 Patent	
	D448	Exhibit 135, Overview vs. Claims of the '759 Patent	
	D449	Exhibit 136, RFC 2401 vs. Claims of the '759 Patent	
	D450	Exhibit 137, Schulzrinne vs. Claims of the '135 Patent	
	D451	Exhibit 138, Schulzrinne vs. Claims of the '151 Patent	
	D452	Exhibit 139, Schulzrinne vs. Claims of the '180 Patent	
	D453	Exhibit 140, Schulzrinne vs. Claims of the '211 Patent	
	D454	Exhibit 141, Schulzrinne vs. Claims of the '504 Patent	
	D455	Exhibit 142, Schulzrinne vs. Claims of the '759 Patent	
	D456	Exhibit 143, Solana vs. Claims of the '135 Patent	
	D457	Exhibit 144, Solana vs. Claims of the '151 Patent	
	D458	Exhibit 145, Solana vs. Claims of the '180 Patent	
	D459	Exhibit 146, Solana vs. Claims of the '211 Patent	
	D460	Exhibit 147, Solana vs. Claims of the '504 Patent	
	D461	Exhibit 148, Solana vs. Claims of the '759 Patent	
	D462	Exhibit 149, Atkinson vs. Claims of the '135 Patent	
	D463	Exhibit 150, Atkinson vs. Claims of the '151 Patent	
	D464	Exhibit 151, Atkinson vs. Claims of the '180 Patent	
	D465	Exhibit 152, Atkinson vs. Claims of the '211 Patent	
	D466	Exhibit 153, Atkinson vs. Claims of the '504 Patent	
	D467	Exhibit 154, Atkinson vs. Claims of the '759 Patent	
	D468	Exhibit 155, Marino 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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D469	Exhibit 156, Marino vs. Claims of the '151 Patent	
	D470	Exhibit 157, Marino vs. Claims of the '180 Patent	
	D471	Exhibit 158, Marino vs. Claims of the '211 Patent	
	D472	Exhibit 159, Marino vs. Claims of the '504 Patent	
	D473	Exhibit 160, Marino vs. Claims of the '759 Patent	
	D474	Exhibit 161, Aziz ('646) vs. Claims of the '759 Patent	
	D475	Exhibit 162, Wesinger vs. Claims of the '135 Patent	
	D476	Exhibit 163, Wesinger vs. Claims of the '151 Patent	
	D477	Exhibit 164, Wesinger vs. Claims of the '180 Patent	
	D478	Exhibit 165, Wesinger vs. Claims of the '211 Patent	
	D479	Exhibit 166, Wesinger vs. Claims of the '504 Patent	
	D480	Exhibit 167, Wesinger vs. Claims of the '759 Patent	
	D481	Exhibit 168, Aziz ('234) vs. Claims of the '135 Patent	
	D482	Exhibit 169, Aziz ('234) vs. Claims of the '151 Patent	
	D483	Exhibit 170, Aziz ('234) vs. Claims of the '180 Patent	
	D484	Exhibit 171, Aziz ('234) vs. Claims of the '211 Patent	
	D485	Exhibit 172, Aziz ('234) vs. Claims of the '504 Patent	
	D486	Exhibit 173, Aziz ('234) vs. Claims of the '759 Patent	
	D487	Exhibit 174, Schneider vs. Claims of the '759 Patent	
	D488	Exhibit 175, Valencia vs. Claims of the '135 Patent	
	D489	Exhibit 176, Valencia vs. Claims of the '151 Patent	
	D490	Exhibit 177, Valencia vs. Claims of the '180 Patent	
	D491	Exhibit 178, Valencia vs. Claims of the '211 Patent	
	D492	Exhibit 179, Valencia vs. Claims of the '504 Patent	
	D493	Exhibit 180, RFC 2401 in Combination with U.S. Patent No. 6,496,867 vs. Claims of the '180 Patent	
	D494	Exhibit 181, Davison vs. Claims of the '135 Patent	
	D495	Exhibit 182, Davison vs. Claims of the '151 Patent	
	D496	Exhibit 183, Davison vs. Claims of the '180 Patent	
	D497	Exhibit 184, Davison vs. Claims of the '211 Patent	
	D498	Exhibit 185, Davison vs. Claims of the '504 Patent	
	D499	Exhibit 186, Davison vs. Claims of the '759 Patent	
	D500	Exhibit 187, AutoSOCKS v2.1 vs. Claims of the '135 Patent	
	D501	Exhibit 188, AutoSOCKS v2.1 vs. Claims of the '151 Patent	
	D502	Exhibit 189, AutoSOCKS v2.1 Administrator's Guide vs. Claims of the '180 Patent	
	D503	Exhibit 190, AutoSOCKS vs. Claims of the '759 Patent	
	D504	Exhibit 191, Aventail Connect 3.01/2.51 vs. Claims of the '135 Patent	
	D505	Exhibit 192, Aventail Connect v3.01/2.51 vs. Claims of the '151 Patent	
	D506	Exhibit 193, Aventail Connect 3.01/2.51 vs. Claims of the '180 Patent	
	D507	Exhibit 194, Aventail Connect 3.01/2.51 vs. Claims of the '759 Patent	
	D508	Exhibit 195, Aventail Connect 3.1/2.6 Administrator's Guide vs. Claims of the '135 Patent	
	D509	Exhibit 196, Aventail Connect 3.1/2.6 Administrator's Guide vs. Claims of the '151 Patent	
	D510	Exhibit 197, Aventail Connect 3.1/2.6 vs. Claims of the '180 Patent	
	D511	Exhibit 198, Aventail Connect 3.1/2.6 vs. Claims of the '759 Patent	
	D512	Exhibit 199, BinGO! User's User's Guide/Extended Features Reference vs. Claims of the '151 Patent	
	D513	Exhibit 200, BinGO! User's User's Guide/Extended Features Reference vs. Claims of the '135 Patent	
	D514	Exhibit 201, BinGO! vs. Claims of the '180 Patent	
	D515	Exhibit 202, BinGO! vs. Claims of the '759 Patent	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D516	Exhibit 203, Broadband Forum Technical Report TR-025 (Issue 1.0/5.0) vs. Claims of the '135 Patent	
	D517	Exhibit 204, Domain Name System (DNS) Security vs. Claims of the '211 Patent	
	D518	Exhibit 205, Domain Name System (DNS) Security vs. Claims of the '504 Patent	
	D519	Exhibit 206, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '211 Patent	
	D520	Exhibit 207, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '504 Patent	
	D521	Exhibit 208, RFC 2538, Storing Certificates in the Domain Name System (DNS) vs. Claims of the '211 Patent	
	D522	Exhibit 209, RFC 2538, Storing Certificates in the Domain Name System (DNS) vs. Claims of the '504 Patent	
	D523	Exhibit 210, IETF RFC 2065: Domain Name System Security Extensions; Published January 1997 vs. Claims of the '504 Patent	
	D524	Exhibit 211, IETF RFC 2065: Domain Name System Security Extensions; Published January 1997 vs. Claims of the '211 Patent	
	D525	Exhibit 212, RFC 2486, RFC 2661, RFC 2401, and Internet-Draft, "Secure Remote Access with L2TP" vs. Claims of the '135 Patent	
	D526	Exhibit 213, U.S. Patent No. 7,100,195 in Combination with RFC 2401 and U.S. Patent No. 6,496,867 vs. Claims of the '135 Patent	
	D527	Exhibit 214, U.S. Patent No. 7,100,195 in Combination with RFC 2401 and U.S. Patent No. 6,496,867 vs. Claims of the '151 Patent	
	D528	Exhibit 215, U.S. Patent No. 6,643,701 vs. Claims of the '135 Patent	
	D529	Exhibit 216, U.S. Patent No. 6,643,701 vs. Claims of the '151 Patent	
	D530	Exhibit 217, U.S. Patent No. 6,496,867 in Combination with RFC 2401 vs. Claims of the '151 Patent	
	D531	Exhibit 218, U.S. Patent No. 6,496,867 in Combination with RFC 2401 vs. Claims of the '135 Patent	
	D532	Exhibit 219, U.S. Patent No. 6,496,867 vs. Claims of the '211 Patent	
	D533	Exhibit 220, U.S. Patent No. 6,496,867 vs. Claims of the '504 Patent	
	D534	Exhibit 221, RFC 2486, RFC 2661, RFC 2401, and Internet-Draft, "Secure Remote Access with L2TP" vs. Claims of the '151 Patent	
	D535	Exhibit 222, U.S. Patent No. 6,557,037 vs. Claims of the '211 Patent	
	D536	Exhibit 223, U.S. Patent No. 6,557,037 vs. Claims of the '504 Patent	
	D537	Exhibit 224, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '135 Patent	
	D538	Exhibit 225, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '151 Patent	
	D539	Exhibit Cisco-1, Cisco's Prior Art Systems vs. Claims of the '135 Patent	
	D540	Exhibit Cisco-2, Cisco's Prior Art Systems vs. Claims of the '151 Patent	
	D541	Exhibit Cisco-3, Cisco's Prior Art Systems vs. Claims of the '180 Patent	
	D542	Exhibit Cisco-4, Cisco's Prior Art Systems vs. Claims of the '211 Patent	
	D543	Exhibit Cisco-5, Cisco's Prior Art Systems vs. Claims of the '504 Patent	
	D544	Exhibit Cisco-6, Cisco's Prior Art Systems vs. Claims of the '759 Patent	
	D545	Exhibit Cisco-7, Cisco's Prior Art PIX System vs. Claims of the '759 Patent	
	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)	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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 *VirnetX 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).	
	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	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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").	
	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: Simpson, 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)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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	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	
	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 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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D660	Exhibit 38, RFC 2661 vs. Claims of the '211 Patent	
	D661	Exhibit 39, RFC 2661 vs. Claims of the '504 Patent	
	D662	Exhibit 40, SecureConnect vs. Claims of the '135 Patent	
	D663	Exhibit 41, SecureConnect vs. Claims of the '211 Patent	
	D664	Exhibit 42, SecureConnect vs. Claims of the '504 Patent	
	D665	Exhibit 43, SFS-HTTP vs. Claims of the '135 Patent	
	D666	Exhibit 44, SFS-HTTP vs. Claims of the '211 Patent	
	D667	Exhibit 45, SFS-HTTP vs. Claims of the '504 Patent	
	D668	Exhibit 46, US '883 vs. Claims of the '135 Patent	
	D669	Exhibit 47, US '883 vs. Claims of the '211 Patent	
	D670	Exhibit 48, US '883 vs. Claims of the '504 Patent	
	D671	Exhibit 49, Chuah vs. Claims of the '135 Patent	
	D672	Exhibit 50, Chuah vs. Claims of the '211 Patent	
	D673	Exhibit 51, Chuah vs. Claims of the '504 Patent	
	D674	Exhibit 52, U.S. '648 vs. Claims of the '135 Patent	
	D675	Exhibit 53, U.S. '648 vs. Claims of the '211 Patent	
	D676	Exhibit 57, B&M VPNs vs. Claims of the '504 Patent	
	D677	Exhibit 58, BorderManager vs. Claims of the '135 Patent	
	D678	Exhibit 59, BorderManager vs. Claims of the '211 Patent	
	D679	Exhibit 60, BorderManager vs. Claims of the '504 Patent	
	D680	Exhibit 61, Prestige 128 Plus vs. Claims of the '135 Patent	
	D681	Exhibit 62, Prestige 128 Plus vs. Claims of the '211 Patent	
	D682	Exhibit 63, Prestige 128 Plus vs. Claims of the '504 Patent	
	D683	Exhibit 64, RFC 2401 vs. Claims of the '135 Patent	
	D684	Exhibit 65, RFC 2401 vs. Claims of the '211 Patent	
	D685	Exhibit 66, RFC 2401 vs. Claims of the '504 Patent	
	D686	Exhibit 67, US '072 vs. Claims of the '135 Patent	
	D687	Exhibit 68, RFC 2486 vs. Claims of the '211 Patent	
	D688	Exhibit 69, RFC 2486 vs. Claims of the '504 Patent	
	D689	Exhibit 70 Understanding IPSec vs. Claims of the '135 Patent	
	D690	Exhibit 71, Understanding IPSec vs. Claims of the '211 Patent	
	D691	Exhibit 72, Understanding IPSec vs. Claims of the '504 Patent	
	D692	Exhibit 73, US '820 vs. Claims of the '135 Patent	
	D693	Exhibit 74, US '820 vs. Claims of the '211 Patent	
	D694	Exhibit 75, US '820 vs. Claims of the '504 Patent	
	D695	Exhibit 76, US '019 vs. Claims of the '211 Patent	
	D696	Exhibit 77, US '019 vs. Claims of the '504 Patent	
	D697	Exhibit 78, US '049 vs. Claims of the '135 Patent	
	D698	Exhibit 79, US '049 vs. Claims of the '211 Patent	
	D699	Exhibit 80, US '049 vs. Claims of the '504 Patent	
	D700	Exhibit 81, US '748 vs. Claims of the '135 Patent	
	D701	Exhibit 82, US '261 vs. Claims of the '135 Patent	
	D702	Exhibit 83, US '261 vs. Claims of the '211 Patent	
	D703	Exhibit 84, US '261 vs. Claims of the '504 Patent	
	D704	Exhibit 85, US '900 vs. Claims of the '135 Patent	
	D705	Exhibit 86, US '900 vs. Claims of the '211 Patent	
	D706	Exhibit 87, US '900 vs. Claims of the '504 Patent	
	D707	Exhibit 88, US '671 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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D708	Exhibit 89, US '671 vs. Claims of the '211 Patent	
	D709	Exhibit 90, US '671 vs. Claims of the '504 Patent	
	D710	Exhibit 91, JP '704 vs. Claims of the '135 Patent	
	D711	Exhibit 92, JP '704 vs. Claims of the '211 Patent	
	D712	Exhibit 93, JP '704 vs. Claims of the '504 Patent	
	D713	Exhibit 94, GB '841 vs. Claims of the '135 Patent	
	D714	Exhibit 95, GB '841 vs. Claims of the '211 Patent	
	D715	Exhibit 96, GB '841 vs. Claims of the '504 Patent	
	D716	Exhibit 97, US '318 vs. Claims of the '135 Patent	
	D717	Exhibit 98, US '318 vs. Claims of the '211 Patent	
	D718	Exhibit 99, US '318 vs. Claims of the '504 Patent	
	D719	Exhibit 100, VPN/VLAN vs. Claims of the '135 Patent	
	D720	Exhibit 101, Nikkei vs. Claims of the '135 Patent	
	D721	Exhibit 102, Nikkei vs. Claims of the '211 Patent	
	D722	Exhibit 103, Nikkei vs. Claims of the '504 Patent	
	D723	Exhibit 104, Special Anthology vs. Claims of the '135 Patent	
	D724	Exhibit 106-A, Gauntlet System vs. Claims of the '135 Patent	
	D725	Exhibit 109-A, Gauntlet System vs. Claims of the '211 Patent	
	D726	Exhibit 110-A, Gauntlet System vs. Claims of the '504 Patent	
	D727	Exhibit 112, IntraPort System vs. Claims of the '135 Patent	
	D728	Exhibit 115, IntraPort System vs. Claims of the '211 Patent	
	D729	Exhibit 116, IntraPort System vs. Claims of the '504 Patent	
	D730	Exhibit 118, Altiga VPN System vs. Claims of the '135 Patent	
	D731	Exhibit 121, Altiga VPN System vs. Claims of the '211 Patent	
	D732	Exhibit 122, Altiga VPN System vs. Claims of the '504 Patent	
	D733	Exhibit 124, Kiuchi vs. Claims of the '135 Patent	
	D734	Exhibit 127, Kiuchi vs. Claims of the '211 Patent	
	D735	Exhibit 128, Kiuchi vs. Claims of the '504 Patent	
	D736	Exhibit 137, Schulzrinne vs. Claims of the '135 Patent	
	D737	Exhibit 137, Schulzrinne vs. Claims of the '135 (Final) Patent	
	D738	Exhibit 140, Schulzrinne vs. Claims of the '211 Patent	
	D739	Exhibit 141, Schulzrinne vs. Claims of the '504 Patent	
	D740	Exhibit 143, Solana vs. Claims of the '135 Patent	
	D741	Exhibit 146, Solana vs. Claims of the '211 Patent	
	D742	Exhibit 147, Solana vs. Claims of the '504 Patent	
	D743	Exhibit 155, Marino vs. Claims of the '135 Patent	
	D744	Exhibit 158, Marino vs. Claims of the '211 Patent	
	D745	Exhibit 159, Marino vs. Claims of the '504 Patent	
	D746	Exhibit 168, Aziz vs. Claims of the '135 Patent	
	D747	Exhibit 171, U.S. '234 vs. Claims of the '211 Patent	
	D748	Exhibit 172, Aziz vs. Claims of the '504 Patent	
	D749	Exhibit 175, Valencia vs. Claims of the '135 Patent	
	D750	Exhibit 178, Valencia vs. Claims of the '211 Patent	
	D751	Exhibit 179, Valencia vs. Claims of the '504 Patent	
	D752	Exhibit 181, Davison vs. Claims of the '135 Patent	
	D753	Exhibit 184, Davison vs. Claims of the '211 Patent	
	D754	Exhibit 185, Davison vs. Claims of the '504 Patent	
	D755	Exhibit 200, BinGO! User's Guide/Extended Features Reference 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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D756	Exhibit 203, Broadband Forum Technical Report TR-025 (Issue 1.0/5.0) vs. Claims of the '135 Patent	
	D757	Exhibit 206, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '211 Patent	
	D758	Exhibit 207, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '504 Patent	
	D759	Exhibit 208, RFC 2538, Storing Certificates in the Domain Name System (DNS) vs. Claims of the '211 Patent	
	D760	Exhibit 209, RFC 2538, Storing Certificates in the Domain Name System (DNS) vs. Claims of the '504 Patent	
	D761	Exhibit 212, RFC 2486, RFC 2661, RFC 2401 and Internet-Draft, "Secure Remote Access with L2TP' vs. Claims of the '135 Patent	
	D762	Exhibit 218, U.S. Patent No. 6,496,867 in combination with RFC 2401' vs. Claims of the '135 Patent	
	D763	Exhibit 219, U.S. Patent No. 6,496,867 vs. Claims of the '211 Patent	
	D764	Exhibit 220, U.S. Patent No. 6,496,867 vs. Claims of the '504 Patent	
	D765	Exhibit 222, U.S. Patent No. 6,557,037 vs. Claims of the '211 Patent	
	D766	Exhibit 223, U.S. Patent No. 6,557,037 vs. Claims of the '504 Patent	
	D767	Exhibit 224, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '135 Patent	
	D768	Exhibit 228, U.S. 588 vs. Claims of the '211 Patent (Final)	
	D769	Exhibit 229, U.S. 588 vs. Claims of the '504 Patent (Final)	
	D770	Exhibit 230, Microsoft VPN vs. Claims of the '135 Patent (Final)	
	D771	Exhibit 231, Microsoft VPN vs. Claims of the '211 Patent (Final)	
	D772	Exhibit XX, Microsoft VPN vs. Claims of the '504 Patent	
	D773	Exhibit Cisco-1, Cisco's Prior Art System vs. Claims of the '135 Patent	
	D774	Exhibit Cisco-4, Cisco's Prior Art System vs. Claims of the '211 Patent	
	D775	Exhibit Cisco-5, Cisco's Prior Art System vs. Claims of the '504 Patent	
	D776	Exhibit 225, US '037 vs. Claims of the '135 Patent	
	D777	Exhibit 226, ITU-T Standardization Activities vs. Claims of the '135 Patent	
	D778	Exhibit 227, US '393 vs. Claims of the '135 Patent	
	D779	Exhibit 233, The Miller Application vs. Claim 13 of the '135 Patent	
	D780	Exhibit 234, Aventail Connect 3.1/2.6 Administrator's Guide ("Aventail Connect") vs. Claims of the '504 Patent	
	D781	Exhibit 235, Microsoft VPN vs. Claims of the '504 Patent	
	D782	Exhibit 1, IETF RFC 2065: Domain Name System Security Extensions; published January 1997 vs. Claims of the '211 Patent	
	D783	Exhibit 2, IETF RFC 2065: Domain Name System Security Extensions; published January 1997 vs. Claims of the '504 Patent	
	D784	Exhibit 3, RFC 2543 vs. Claims of the '135 Patent	
	D785	Exhibit 4, RFC 2543 vs. Claims of the '211 Patent	
	D786	Exhibit 5, RFC 2543 vs. Claims of the '504 Patent	
	D787	Exhibit 6, SIP Draft v.2 vs. Claims of the '135 Patent	
	D788	Exhibit 7, SIP Draft v.2 vs. Claims of the '211 Patent	
	D789	Exhibit 8, SIP Draft v.2 vs. Claims of the '504 Patent	
	D790	Exhibit 9, H.323 vs. Claims of the '135 Patent	
	D791	Exhibit 10, H.323 vs. Claims of the '211 Patent	
	D792	Exhibit 11, H.323 vs. Claims of the '504 Patent	
	D793	Exhibit 12, SSL 3.0 vs. Claims of the '135 Patent	
	D794	Exhibit 13, SSL 3.0 vs. Claims of the '211 Patent	
	D795	Exhibit 14, SSL 3.0 vs. Claims of the '504 Patent	
	D796	Exhibit 15, RFC 2487 vs. Claims of the '135 Patent	
	D797	Exhibit 16, RFC 2487 vs. Claims of the '211 Patent	
	D798	Exhibit 17, RFC 2487 vs. Claims of the '504 Patent	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D799	Exhibit 18, RFC 2595 vs. Claims of the '135 Patent	
	D800	Exhibit 21, iPass vs. Claims of the '135 Patent	
	D801	Exhibit 22, iPass vs. Claims of the '211 Patent	
	D802	Exhibit 23, iPass vs. Claims of the '504 Patent	
	D803	Exhibit 24, U.S. Patent No. 6,453,034 ('034 Patent") vs. Claims of the 135 Patent	
	D804	Exhibit 25, U.S. Patent No. 6,453,034 ('034 Patent") vs. Claims of the 211 Patent	
	D805	Exhibit 26, U.S. Patent No. 6,453,034 ('034 Patent") vs. Claims of the 504 Patent	
	D806	Exhibit 27, U.S. Patent No. 6,223,287 ("287 Patent") vs. Claims of the 135 Patent	
	D807	Exhibit 28, U.S. Patent No. 6,223,287 ("287 Patent") vs. Claims of the 211 Patent	
	D808	Exhibit 29, U.S. Patent No. 6,223,287 ("287 Patent") vs. Claims of the 504 Patent	
	D809	Exhibit 35, RFC 1928 vs. Claims of the '211 Patent	
	D810	Exhibit 36, RFC 1928 vs. Claims of the '504 Patent	
	D811	Exhibit 106, Gaunlet System and Gaunlet References vs. Claims of the '135 Patent	
	D812	Exhibit 109, Gaunlet System and Gaunlet References vs. Claims of the '211 Patent	
	D813	Exhibit 110, Gaunlet System vs. Claims of the '504 Patent	
	D814	Exhibit 130, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '135 Patent	
	D815	Exhibit 133, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '211 Patent	
	D816	Exhibit 134, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '504 Patent	
	D817	Exhibit 149, Atkinson vs. Claims of the '135 Patent	
	D818	Exhibit 152, Atkinson vs. Claims of the '211 Patent	
	D819	Exhibit 153, Atkinson vs. Claims of the '504 Patent	
	D820	Exhibit 162, Wesinger vs. Claims of the '135 Patent	
	D821	Exhibit 165, Wesinger vs. Claims of the '211 Patent	
	D822	Exhibit 166, Wesinger vs. Claims of the '504 Patent	
	D823	Exhibit 187, AutoSOCKS v2.1 vs. Claims of the '135 Patent	
	D824	Exhibit 191, Aventail Connect 3.01/2.51 ("Aventail Connect") vs. Claims of the '135 Patent	
	D825	Exhibit 195, Aventail Connect 3.1/2.6 Administrator's Guide ("Aventail Connect") vs. Claims of the '135 Patent	
	D826	Exhibit 204, Domain Name System (DNS) Security vs. Claims of the '211 Patent	
	D827	Exhibit 205, Domain Name System (DNS) Security ("DNS Security") vs. Claims of the '504 Patent	
	D828	Exhibit 210, Lendenmann vs. Claims of the '211 Patent	
	D829	Exhibit 211, Lendenmann vs. Claims of the '504 Patent	
	D830	Exhibit 213, U.S. Patent No. 7,100,195 in combination with RFC 2401 and U.S. Patent No. 6,496,867 vs. Claims of the '135 Patent	
	D831	Exhibit 215, Aziz vs. Claims of the '135 Patent	
	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)	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D840	Exhibit D7, "Schimpf"; Brian C. Schimpf, "Securing Web Access with DCE," Presented at Network and Distributed System Security (Feb. 10-11, 1997)	
	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"	
	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").	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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	
	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	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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	
	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 vs. Claims of the '135 Patent	
	D911	Exhibit 227, Securing Web Access with DCE vs. Claims of the '151 Patent	
	D912	Exhibit 228, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '135 Patent	
	D913	Exhibit 229, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '151 Patent	
	D914	Exhibit 230, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '180 Patent	
	D915	Exhibit 231, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '211 Patent	
	D916	Exhibit 232, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '504 Patent	
	D917	Exhibit 233, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '759 Patent	
	D918	Exhibit 234, U.S. '648 vs. Claims of the '135 Patent	
	D919	Exhibit 235, U.S. '648 vs. Claims of the '211 Patent	
	D920	Exhibit 236, U.S. '648 vs. Claims of the '504 Patent	
	D921	Exhibit 237, U.S. '648 vs. Claims of the '135 Patent	
	D922	Exhibit 238, Gauntlet System vs. Claims of the '211 Patent	
	D923	Exhibit 239, Gauntlet System vs. Claims of the '504 Patent	
	D924	Exhibit 240, Gauntlet System vs. Claims of the '135 Patent	
	D925	Exhibit 241, U.S. '588 vs. Claims of the '211 Patent	
	D926	Exhibit 242, U.S. '588 vs. Claims of the '504 Patent	
	D927	Exhibit 243, Microsoft VPN vs. Claims of the '135 Patent	
	D928	Exhibit 244, Microsoft VPN vs. Claims of the '211 Patent	
	D929	Exhibit 245, Microsoft VPN vs. Claims of the '504 Patent	
	D930	Exhibit 246, ITU-T Standardization Activities vs. Claims of the '135 Patent	
	D931	Exhibit 247, U.S. '393 vs. Claims of the '135 Patent	
	D932	Exhibit 248, The Miller Application vs. Claim 13 of the '135 Patent	
	D933	Exhibit 249, Gauntlet System vs. Claims of the '151 Patent	
	D934	Exhibit 250, ITU-T Standardization Activities vs. Claims of the '151 Patent	
	D935	Exhibit 251, U.S. Patent No. 5,940,393 vs. Claims of the '151 Patent	
	D936	Exhibit 252, Microsoft VPN vs. Claims of the '151 Patent	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D937	Exhibit 253, U.S. Patent No.6,324,648 vs. Claims of the '151 Patent	
	D938	Exhibit 254, U.S. Patent No.6,857,072 vs. Claims of the '151 Patent	
	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	
	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	PTO Form 1449	
	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	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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	
	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	PTO Form 1449	
	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	
	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	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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	
	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	PTO Form 1449	
	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	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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	
	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 vs. Claims of the '135 Patent	
	D1056	Exhibit 227, Securing Web Access with DCE vs. Claims of the '151 Patent	
	D1057	Exhibit 228, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '135 Patent	
	D1058	Exhibit 229, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '151 Patent	
	D1059	Exhibit 230, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '180 Patent	
	D1060	Exhibit 231, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '211 Patent	
	D1061	Exhibit 232, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '504 Patent	
	D1062	Exhibit 233, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '759 Patent	
	D1063	Exhibit 234, U.S. '648 vs. Claims of the '135 Patent	
	D1064	Exhibit 235, U.S. '648 vs. Claims of the '211 Patent	
	D1065	Exhibit 236, U.S. '648 vs. Claims of the '504 Patent	
	D1066	Exhibit 237, U.S. '072 vs. Claims of the '135 Patent	
	D1067	Exhibit 238, Gauntlet System vs. Claims of the '211 Patent	
	D1068	Exhibit 239, Gauntlet System vs. Claims of the '504 Patent	
	D1069	Exhibit 240, Gauntlet System vs. Claims of the '135 Patent	
	D1070	Exhibit 241, U.S. '588 vs. Claims of the '211 Patent	
	D1071	Exhibit 242, U.S. '588 vs. Claims of the '504 Patent	
	D1072	Exhibit 243, Microsoft VPN vs. Claims of the '135 Patent	
	D1073	Exhibit 244, Microsoft VPN vs. Claims of the '211 Patent	
	D1074	Exhibit 245, Microsoft VPN vs. Claims of the '504 Patent	
	D1075	Exhibit 246, ITU-T Standardization Activities vs. Claims of the '135 Patent	
	D1076	Exhibit 247, U.S. '393 vs. Claims of the '135 Patent	
	D1077	Exhibit 248, The Miller Application vs. Claim 13 of the '135 Patent	
	D1078	Exhibit 249, Gauntlet System vs. Claims of the '151 Patent	
	D1079	Exhibit 250, ITU-T Standardization Activities vs. Claims of the '151 Patent	
	D1080	Exhibit 251, U.S. Patent No. 5,940,393 vs. Claims of the '151 Patent	
	D1081	Exhibit 252, Microsoft VPN vs. Claims of the '151 Patent	
	D1082	Exhibit 253, U.S. Patent No.6,324,648 vs. 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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1083	Exhibit 254, U.S. Patent No.6,857,072 vs. Claims of the '151 Patent	
	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	
	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)	
	D1112	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	
	D1113	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	
	D1114	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	
	D1115	ITU-T Recommendation H.245, "Infrastructure of Audiovisual Services – Communication Procedures. Control Protocol for Multimedia Communication," International Telecommunication Union, pages 1-280, February 1998	
	D1116	Request for Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No.8,051,181)	
	D1117	Transmittal Letters (Patent No.8,051,181)	
	D1118	Exhibit X5, Droms, R., RFC 2131, "Dynamic Host Configuration Protocol," 1987	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1119	Hopen Transcript dated April 11, 2012	
	D1120	VirnetX Claim Construction Opinion	
	D1121	Declaration of Angelos D. Keromytic, Ph.D.	
	D1122	Declaration of Dr. Robert Dunham Short III	
	D1123	Exhibit A-1, Verdict Form from VirnetX, Inc. v. Microsoft Corp., No. 6:07-CV-80 (E.D. Tex.)	
	D1124	Exhibit A-3, Declaration of Jason Nieh, Ph.D. (Control No. 95/001,269)	
	D1125	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	
	D1126	Exhibit B-1, Excerpt from Deposition of Defense FY 2000/2001 Biennial Budget Estimates, Feb. 1999	
	D1127	Exhibit B-2, Collection of Reports and Presentations on DARPA Projects	
	D1128	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	
	D1129	Joel Snyder, Living in Your Own Private Idaho, Network World (January 28, 1998) http://www.networkworld.com/intranet/0126review.html.	
	D1130	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	
	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. 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]	
	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]	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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	
	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	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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	
	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	
	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	
	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)	
	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	
	D1215	Alexander Invalidity Expert Report dtd May 22, 2012 with Exhibits	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1216	Deposition of Peter Alexander dtd July 27, 2012	
	D1217	Cisco '151 Comments by Third Party Requester dtd August 17, 2012 with Exhibits	
	D1218	Cisco '151 Petition to Waive Page Limit Requirement for Third Party Comments dtd August August 17, 2012	
	D1219	Deposition of Stuart Stubblebine dtd August 22, 2012	
	D1220	Defendants' Motion For Reconsideration of the Construction of the Term "Secure Communication Link," 7 pages, June 2012	
	D1221	Green, "Cisco Leverages Altiga Technology for VPN's," 2 pages, 2000 http://www.crn.com/news/channel-programs/18807923/cisco-leverages-altiga-technology-for-vpns.htm	
	D1222	Altiga Networks Archived at http://web.archive.org/web/20000823023437/http:/www.altiga.com/products/ 1999 and Retrieved by the Wayback Machine	
	D1223	Kiuchi, "C-HTTP The Development of a Secure, Closed HTTP-Based Network on the Internet," Department of Epidemiology and Biostatistics, Faculty of Medicine, University of Tokyo, Japan	
	D1224	Lee et al., "Uniform Resource Locators (URL)," Network Working Group, RFC 1738, December 1994 (25 pages)	
	D1225	VPN 3000 Concentrator Series, User Guide; Release 2.5 July 2000 (489 pages)	
	D1226	VPN 3000 Concentrator Series, Getting Started; Release 2.5 July 2000 (122 pages)	
	D1227	Fratto, Altiga Concentrates on VPN Security (Hardware Review Evaluation), Network Computing, March 22, 1999 (2 pages)	
	D1228	Response to RFP: Altiga, Network World Fusion, May 10, 1999 (7 pages)	
	D1229	Altiga Proves Multi-Vendor Interoperability for Seamless VPN Deployment; VPN Workshop Marks Significant Development in the VPN Market, July 12, 1999 (2 pages)	
	D1230	Altiga VPN Concentrator Series (C50) Versus Nortel Networks Contivity Extranet Switch 4000 and 4500, VPN Tunneling competitive Evaluation, 1999 (6 pages)	
	D1231	VPN 3000 Client User Guide, Release 2.5, July 2000 (94 pages)	
	D1232	Digital Certificates Design Specification for Release 2.0, May 17, 1999 (21 pages)	
	D1233	Altiga IPSec Client Architecture, Revision 1.0, April 5, 1999 (34 pages)	
	D1234	Altiga IPSec Functional Specification, Revision 2.1, (17 pages)	
	D1235	Altiga Product Requirements, Revision 1.7, May 26, 1998 (17 pages)	
	D1236	Altiga Network Lists Feature Functional Specification, Revision 1.0, (7 pages)	
	D1237	Altiga Split Tunneling Functional/Design Specification, (15 pages)	
	D1238	Altiga Digital Certificate Support for IPSec Client V2.1 Functional Specification, August 12, 1999 (24 pages)	
	D1239	Altiga IPSec LAN to LAN Tunnel Autodiscovery Functional Specification, (5 pages)	
	D1240	Altiga Split Tunneling Testplan, Revision 1.0, (8 pages)	
	D1241	Altiga VPN Concentrator Getting Started, Revision 1, March 1999 (116 pages)	
	D1242	Altiga VPN Concentrator Getting Started, Version 2, June 1999 (102 pages)	
	D1243	Altiga VPN Concentrator Getting Started, Version 3, December 1999 (130 pages)	
	D1244	Altiga VPN Concentrator Getting Started, Version 4, March 2000 (138 pages)	
	D1245	Altiga VPN Concentrator User Guide, Revision 1, March 1999 (304 pages)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1246	Altiga VPN Concentrator User Guide, Revision 1.1, March 1999 (304 pages)	
	D1247	Altiga VPN Concentrator User Guide, Version 3, June 1999 (478 pages)	
	D1248	Altiga VPN Concentrator User Guide, Version 4, December 1999 (472 pages)	
	D1249	Altiga VPN Concentrator User Guide, Version 5, March 2000 (606 pages)	
	D1250	Altiga VPN Client Installation and User Guide, Version 2, July 1999 (92 pages)	
	D1251	Altiga VPN Concentrator VPN Client Installation and User Guide, Version 3, December 1999 (113 pages)	
	D1252	Altiga VPN Concentrator VPN Client Installation and User Guide, Version 4, March 2000 (118 pages)	
	D1253	Altiga Networks VPN Concentrator and VPN Client, as well as their Public Demonstrations and Testing, are also Described in Marketing Materials and Publications (4 pages)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

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.

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, 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 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.

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[X] 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.

[ ] 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: October 22, 2012

Toby H. Kusmer;Reg. No.:26,418
McDermott Will & Emery L.L.P.
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

Electronic Acknowledgement Receipt

EFS ID:	14053382
Application Number:	13615557
International Application Number:	
Confirmation Number:	1089
Title of Invention:	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:	077580-0177
Receipt Date:	23-OCT-2012
Filing Date:	13-SEP-2012
Time Stamp:	14:33:26
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	1730115 4785032a26ad36a05e57a2080e1cd30457114de6	no	44

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	
Total Files Size (in bytes):	1730115

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.: 077580-0177 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Customer Number: 23630
Victor Larson, et al.	:	Confirmation Number: 1089
Application No.: 13/615,557	:	Group Art Unit: 2447
Filed: September 13, 2012	:	Examiner: Not yet assigned

For: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE TO NOTICE TO FILE CORRECTED APPLICATION PAPERS

Sir:

In response to the Notice To File Corrected Application Papers dated October 4, 2012, submitted herewith are the following for filing in the above-referenced application:

1. Replacement Abstract; and
2. Replacement Drawings (clean without copy marks) for Figures 1-37 for filing in the above-referenced application. No new matter is believed to have been added to the application by way of the Replacement Drawings.

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 No. 501133 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Date: November 21, 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

REPLACEMENT ABSTRACT

A method is used to transparently create an encrypted communications channel between a client device and a target device. Each device is configured to allow audio/video communications between the client and target devices over the encrypted communications channel once the encrypted communications channel is created. The method comprises receiving from the client device a request for a network address associated with the target device, determining whether the request is requesting access to a device that accepts an encrypted channel connection with the client device, and in response to determining that the request is requesting access to a device that accepts an encrypted communications channel connection with the client device, providing provisioning information required to initiate the creation of the encrypted communications channel between the client device and the target device such that the encrypted communications channel supports secure audio/video communications transmitted between the two devices.

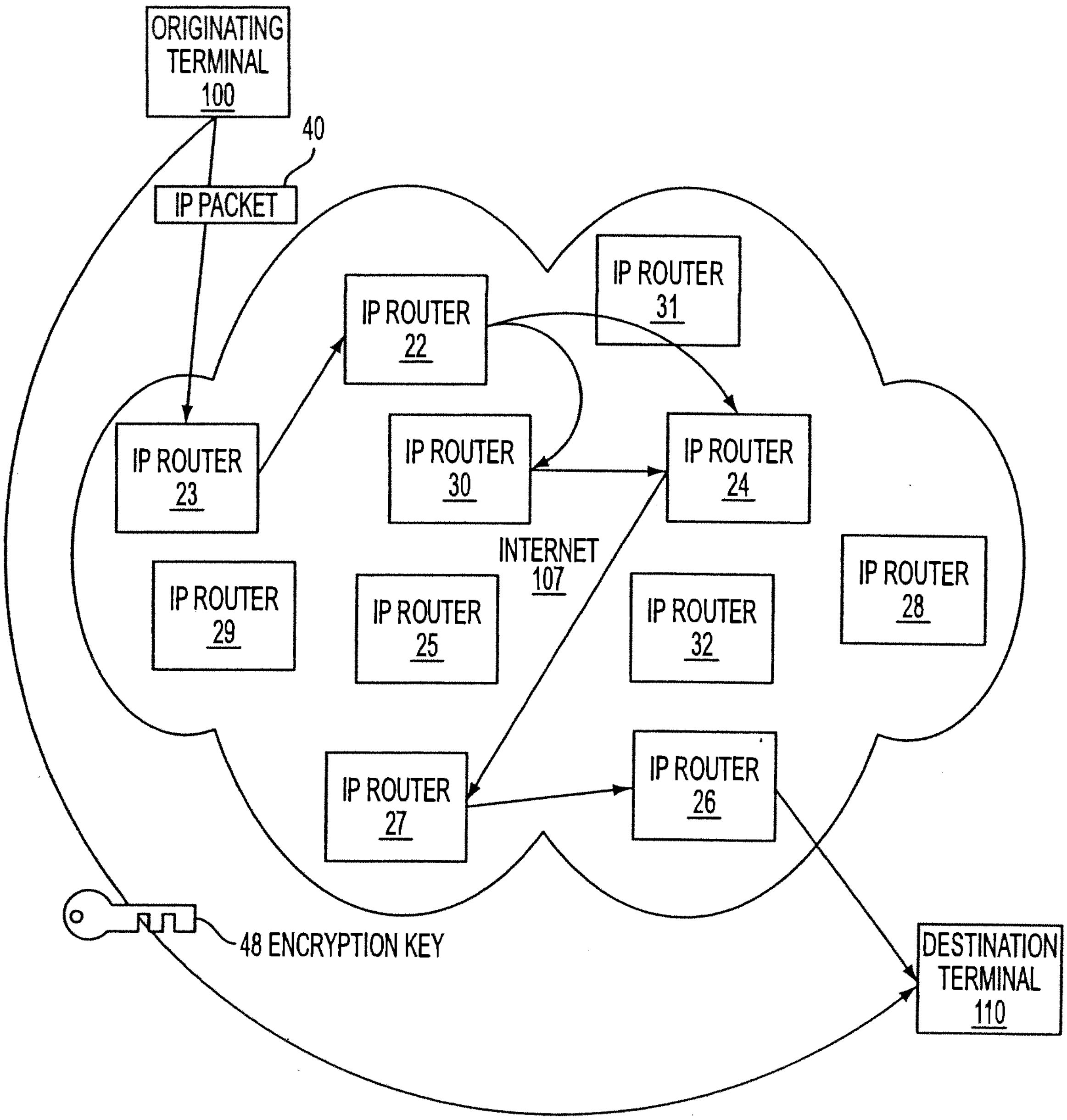

ORIGINATING TERMINAL 100
40
IP PACKET
IP ROUTER 22
IP ROUTER 31
IP ROUTER 23
IP ROUTER 30
IP ROUTER 24
INTERNET 107
IP ROUTER 29
IP ROUTER 25
IP ROUTER 32
IP ROUTER 28
IP ROUTER 27
IP ROUTER 26
48 ENCRYPTION KEY
DESTINATION TERMINAL 110

FIG. 1

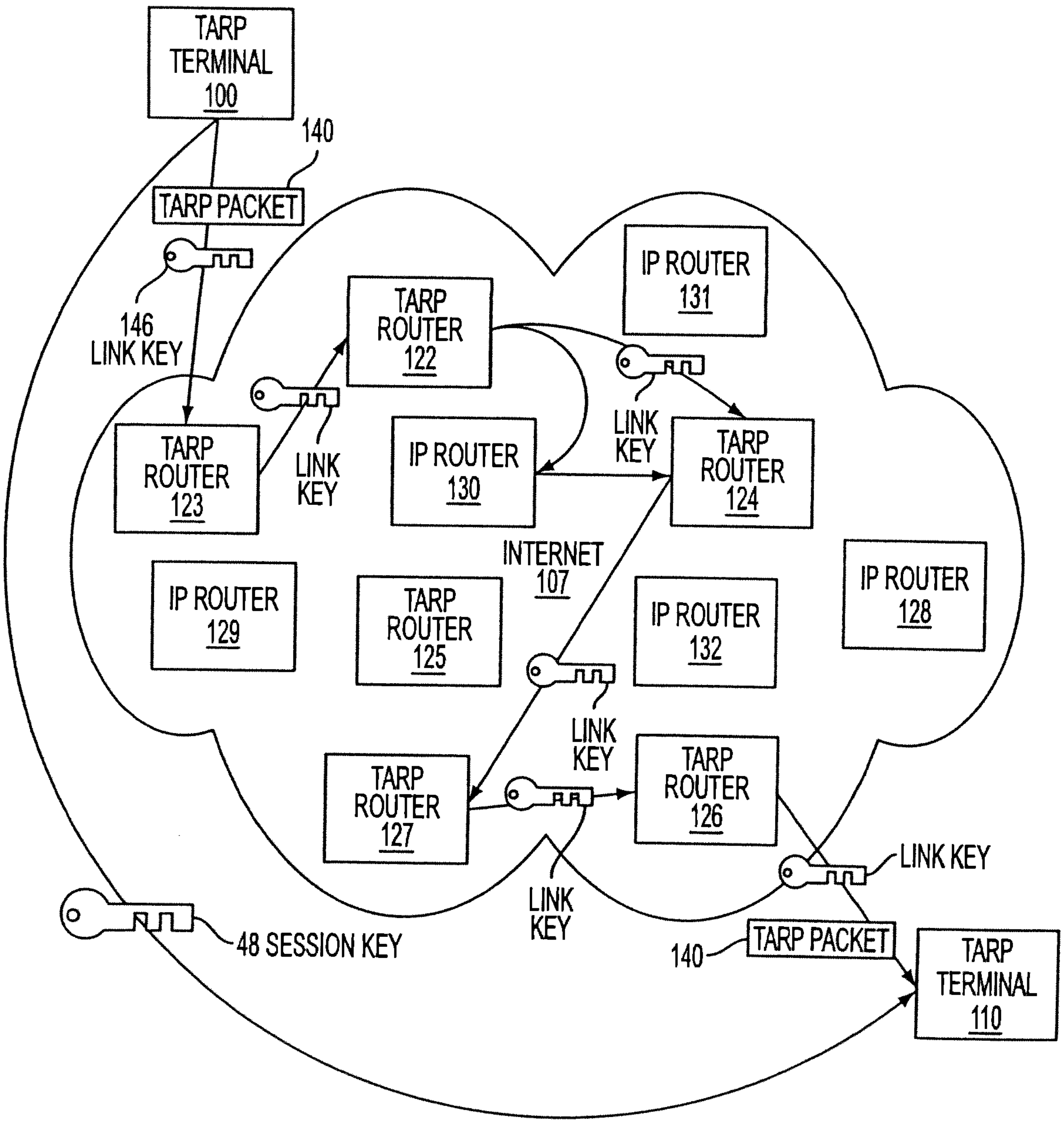

TARP TERMINAL 100
140
TARP PACKET
146 LINK KEY
TARP ROUTER 122
IP ROUTER 131
LINK KEY
TARP ROUTER 123
LINK KEY
IP ROUTER 130
LINK KEY
TARP ROUTER 124
INTERNET 107
IP ROUTER 129
TARP ROUTER 125
IP ROUTER 132
IP ROUTER 128
LINK KEY
TARP ROUTER 127
TARP ROUTER 126
LINK KEY
LINK KEY
48 SESSION KEY
140
TARP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

FIG. 2

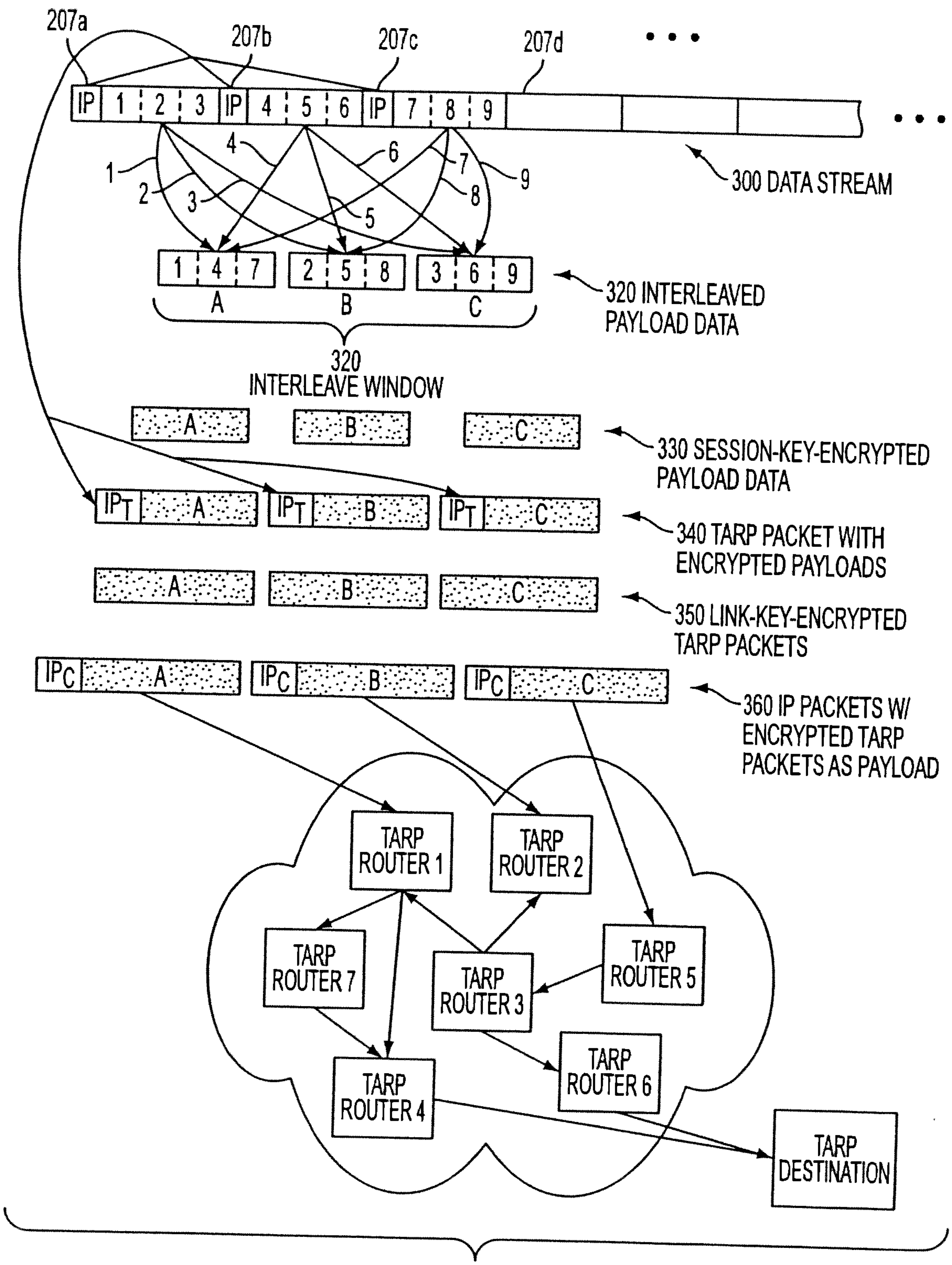
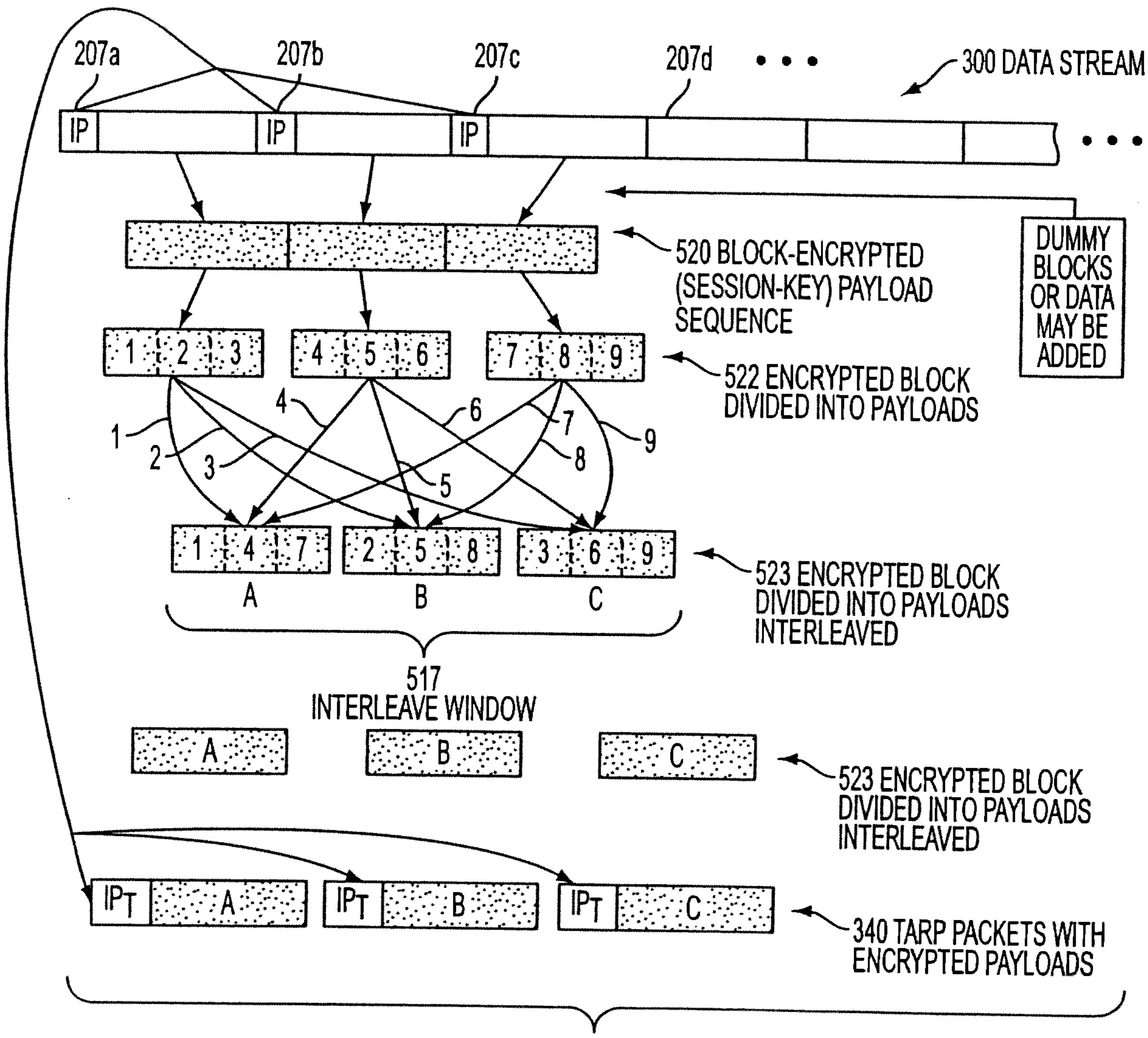

207a
207b
207c
207d
IP 1 2 3 IP 4 5 6 IP 7 8 9
300 DATA STREAM
1 4 7
2 5 8
3 6 9
A B C
320 INTERLEAVED PAYLOAD DATA
320 INTERLEAVE WINDOW
330 SESSION-KEY-ENCRYPTED PAYLOAD DATA
IPT A IPT B IPT C
340 TARP PACKET WITH ENCRYPTED PAYLOADS
350 LINK-KEY-ENCRYPTED TARP PACKETS
IPC A IPC B IPC C
360 IP PACKETS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

FIG. 3B

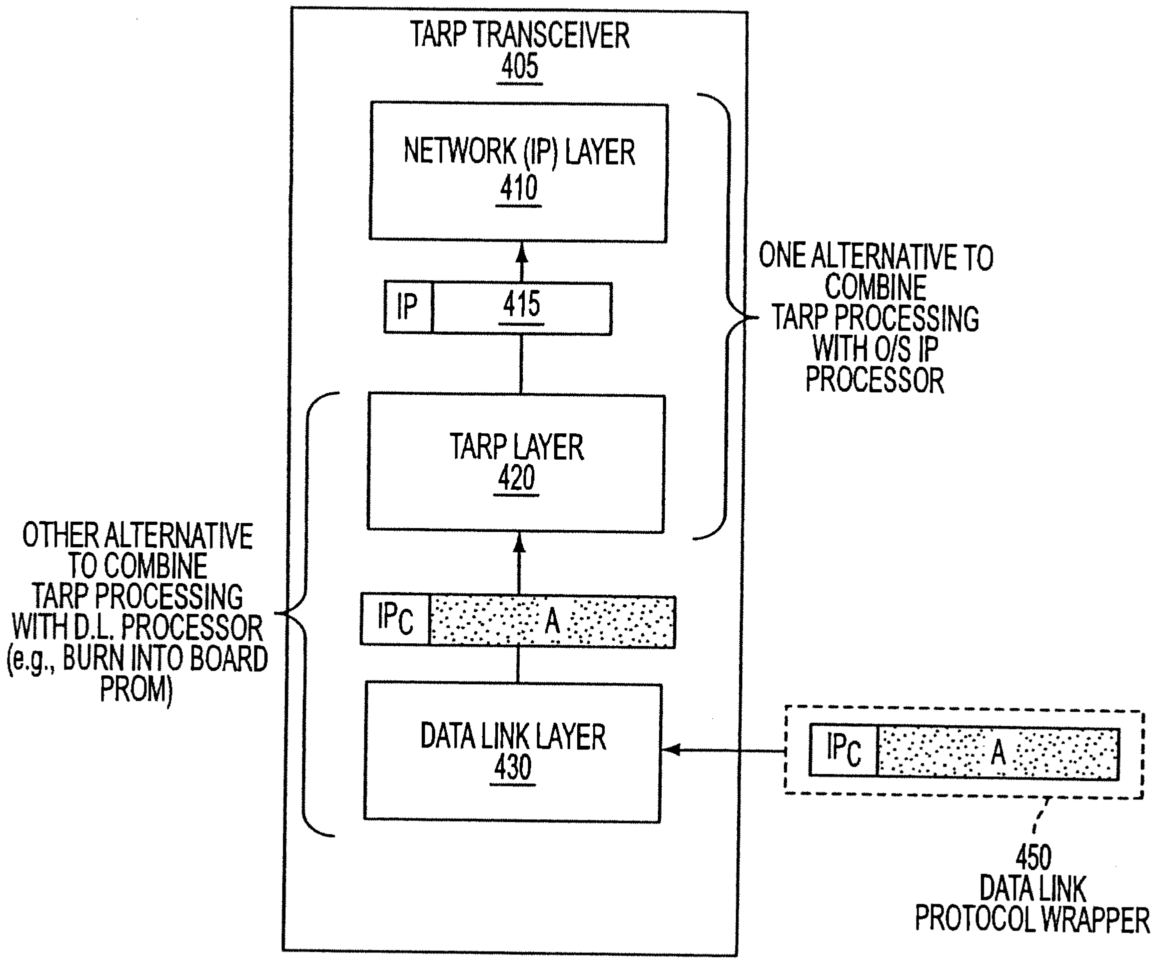

TARP TRANSCEIVER
405
NETWORK (IP) LAYER
410
IP
415
TARP LAYER
420
IPC
A
DATA LINK LAYER
430
ONE ALTERNATIVE TO COMBINE TARP PROCESSING WITH O/S IP PROCESSOR
OTHER ALTERNATIVE TO COMBINE TARP PROCESSING WITH D.L. PROCESSOR (e.g., BURN INTO BOARD PROM)
IPC
A
450
DATA LINK PROTOCOL WRAPPER

FIG. 4

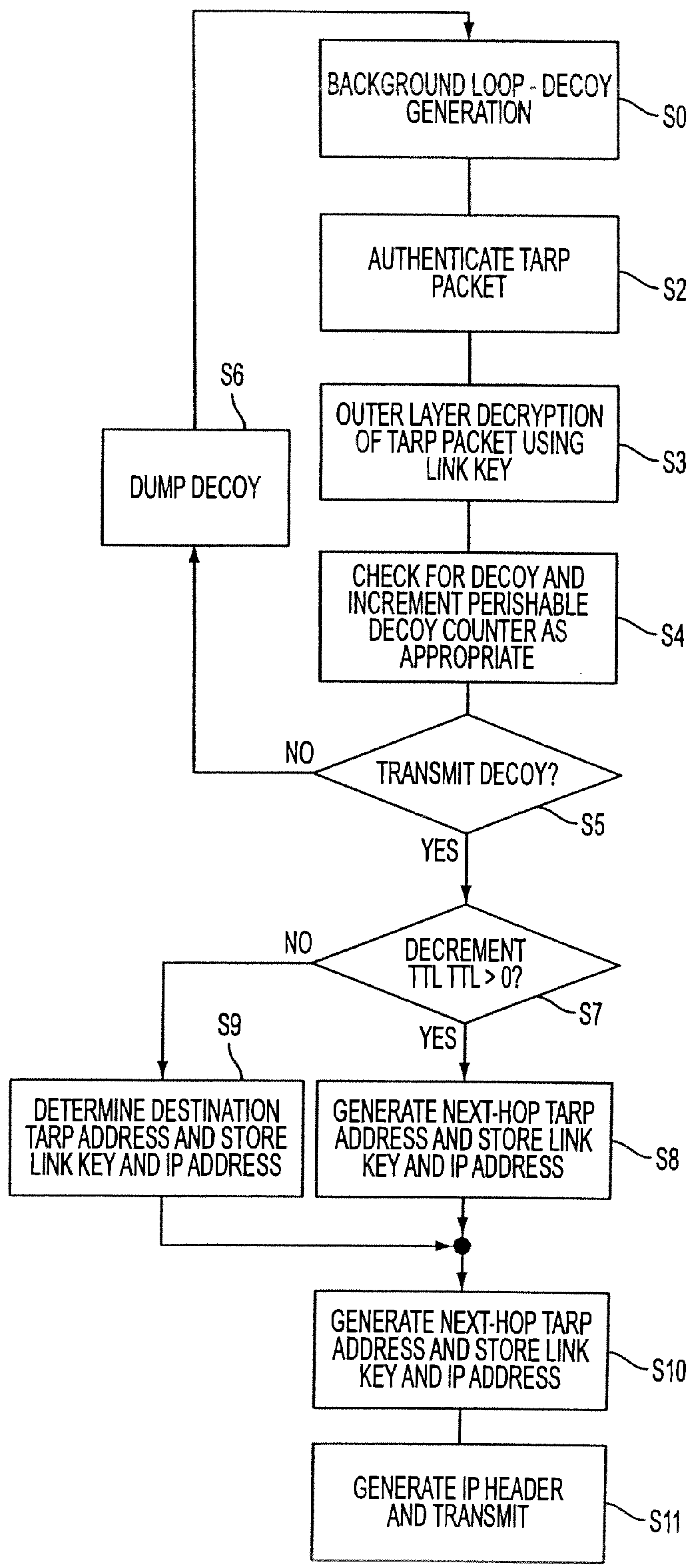

BACKGROUND LOOP - DECOY GENERATION
S0
AUTHENTICATE TARP PACKET
S2
OUTER LAYER DECRYPTION OF TARP PACKET USING LINK KEY
S3
CHECK FOR DECOY AND INCREMENT PERISHABLE DECOY COUNTER AS APPROPRIATE
S4
TRANSMIT DECOY?
S5
NO
YES
DUMP DECOY
S6
DECREMENT TTL TTL > 0?
S7
NO
YES
DETERMINE DESTINATION TARP ADDRESS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

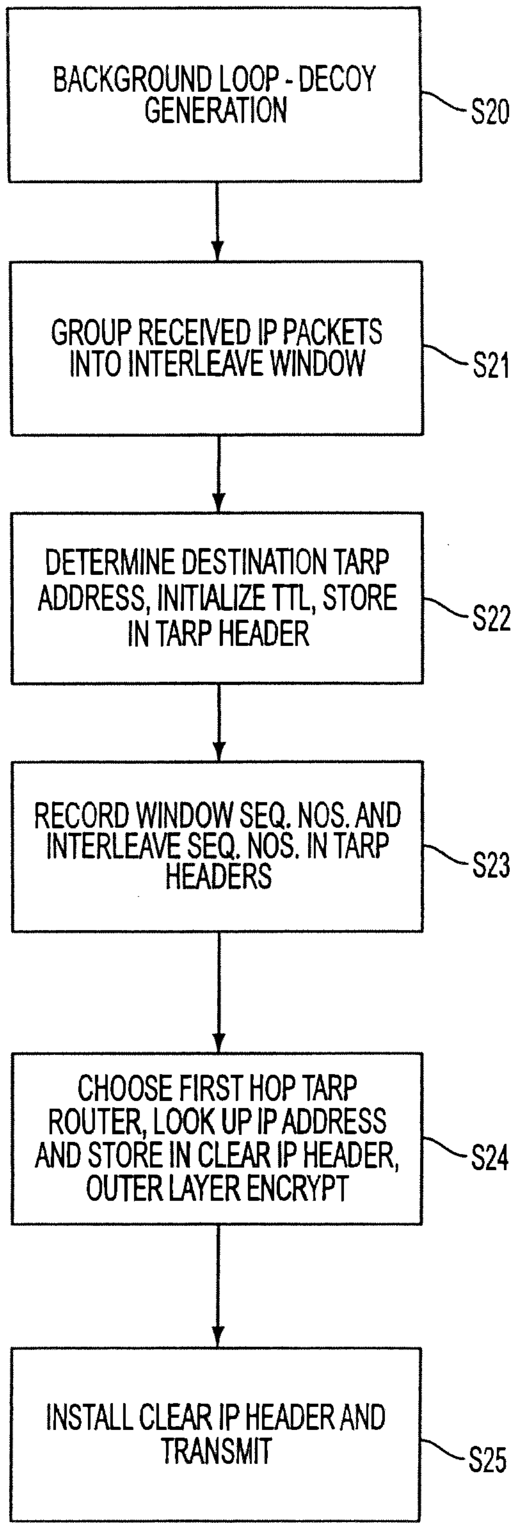

BACKGROUND LOOP - DECOY GENERATION
S20
GROUP RECEIVED IP PACKETS INTO INTERLEAVE WINDOW
S21
DETERMINE DESTINATION TARP ADDRESS, INITIALIZE TTL, STORE IN TARP HEADER
S22
RECORD WINDOW SEQ. NOS. AND INTERLEAVE SEQ. NOS. IN TARP HEADERS
S23
CHOOSE FIRST HOP TARP ROUTER, LOOK UP IP ADDRESS AND STORE IN CLEAR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

FIG. 6

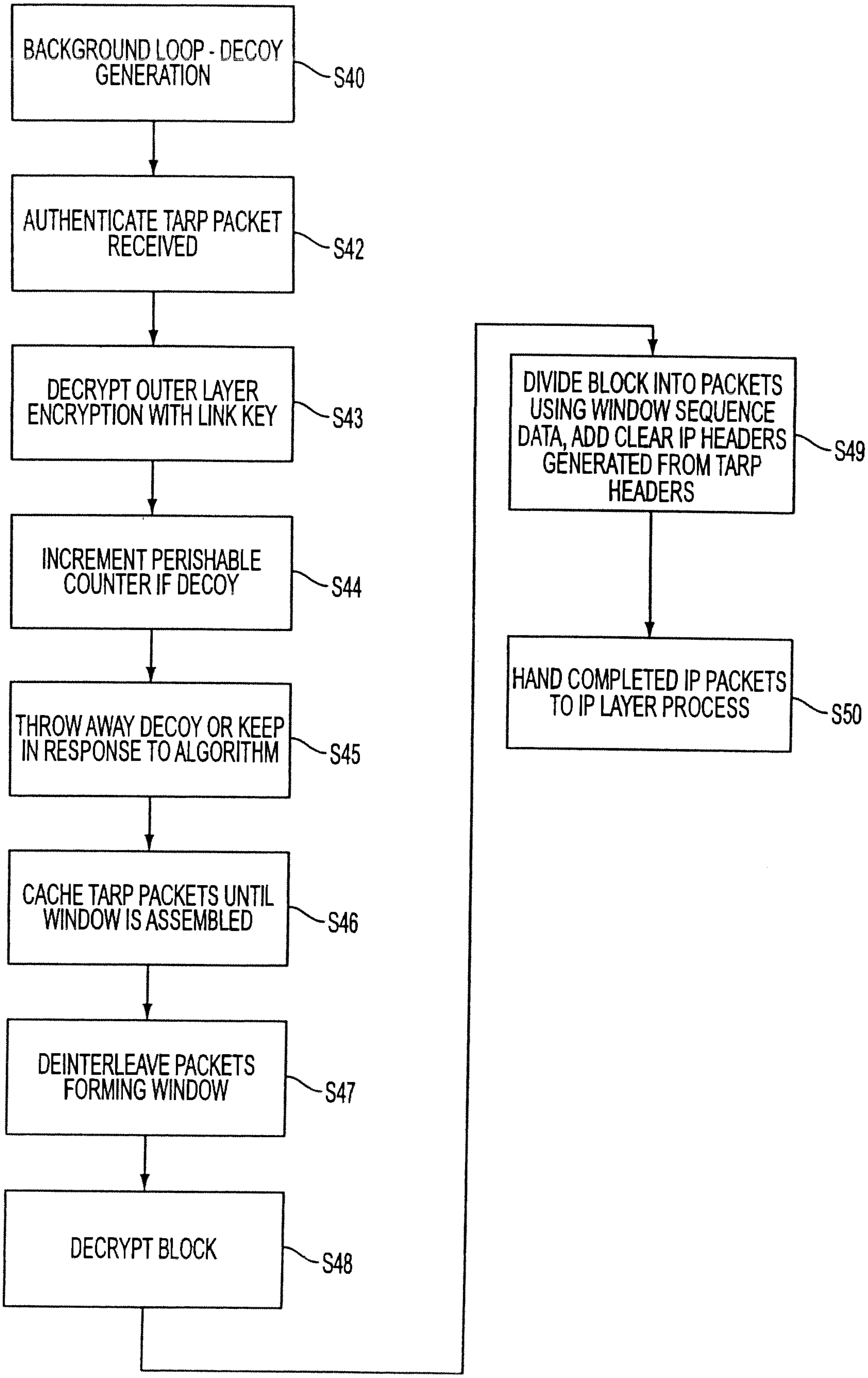

BACKGROUND LOOP - DECOY GENERATION
S40
AUTHENTICATE TARP PACKET RECEIVED
S42
DECRYPT OUTER LAYER ENCRYPTION WITH LINK KEY
S43
INCREMENT PERISHABLE COUNTER IF DECOY
S44
THROW AWAY DECOY OR KEEP IN RESPONSE TO ALGORITHM
S45
CACHE TARP PACKETS UNTIL WINDOW IS ASSEMBLED
S46
DEINTERLEAVE PACKETS FORMING WINDOW
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

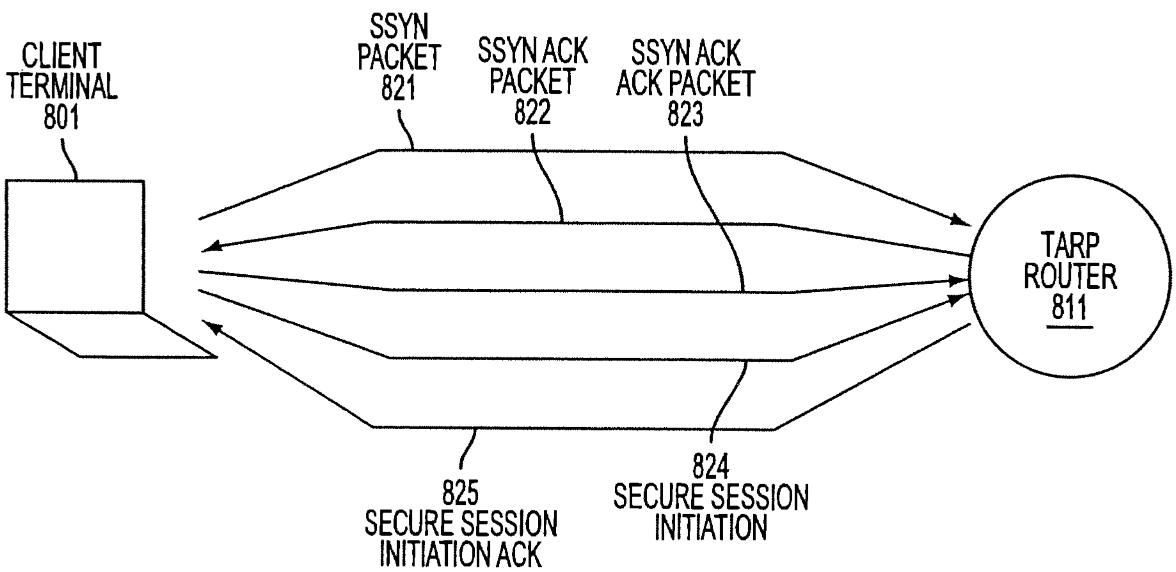
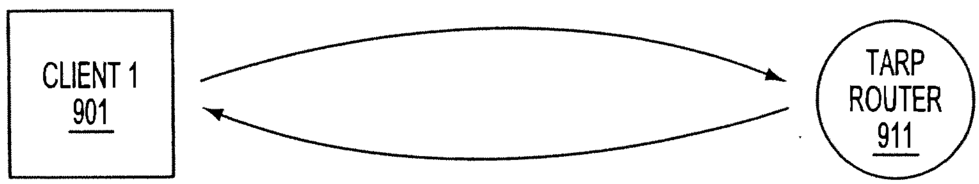

CLIENT
TERMINAL
801
SSYN
PACKET
821
SSYN ACK
PACKET
822
SSYN ACK
ACK PACKET
823
TARP
ROUTER
811
825
SECURE SESSION
INITIATION ACK
824
SECURE SESSION
INITIATION

FIG. 8



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

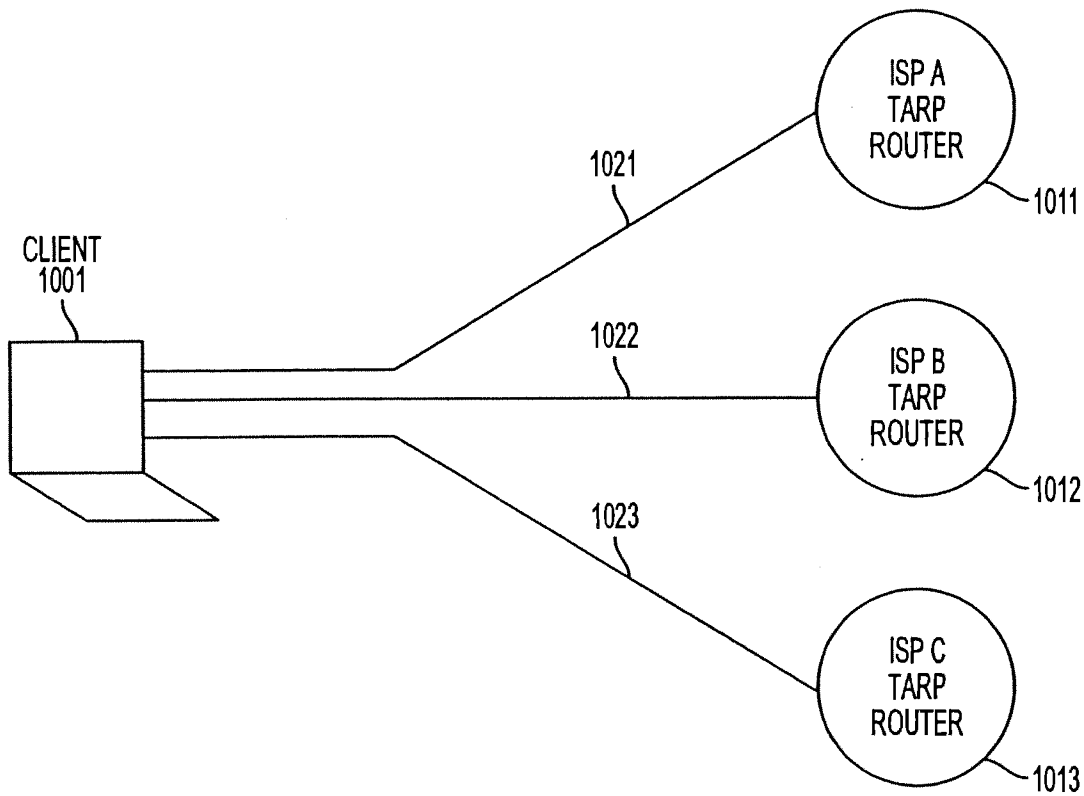

ISP A
TARP
ROUTER
1021
1011
CLIENT
1001
1022
ISP B
TARP
ROUTER
1012
1023
ISP C
TARP
ROUTER
1013

FIG. 10

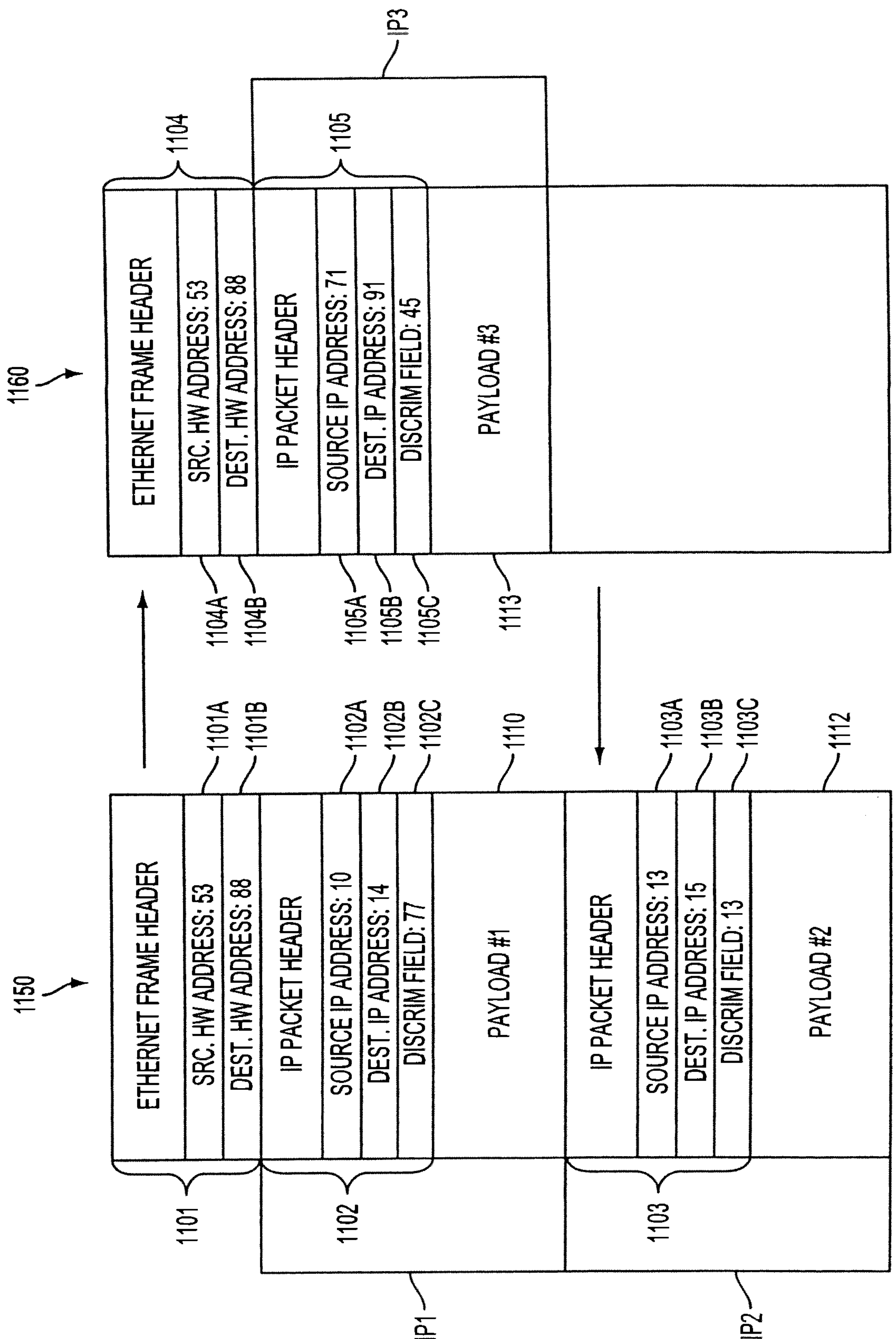

1150
1160
ETHERNET FRAME HEADER
SRC. HW ADDRESS: 53
DEST. HW ADDRESS: 88
IP PACKET HEADER
SOURCE IP ADDRESS: 10
DEST. IP ADDRESS: 14
DISCRIM FIELD: 77
PAYLOAD #1
IP PACKET HEADER
SOURCE IP ADDRESS: 13
DEST. IP ADDRESS: 15
DISCRIM FIELD: 13
PAYLOAD #2
1101
1102
1103
IP1
IP2
1101A
1101B
1102A
1102B
1102C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

FIG. 11

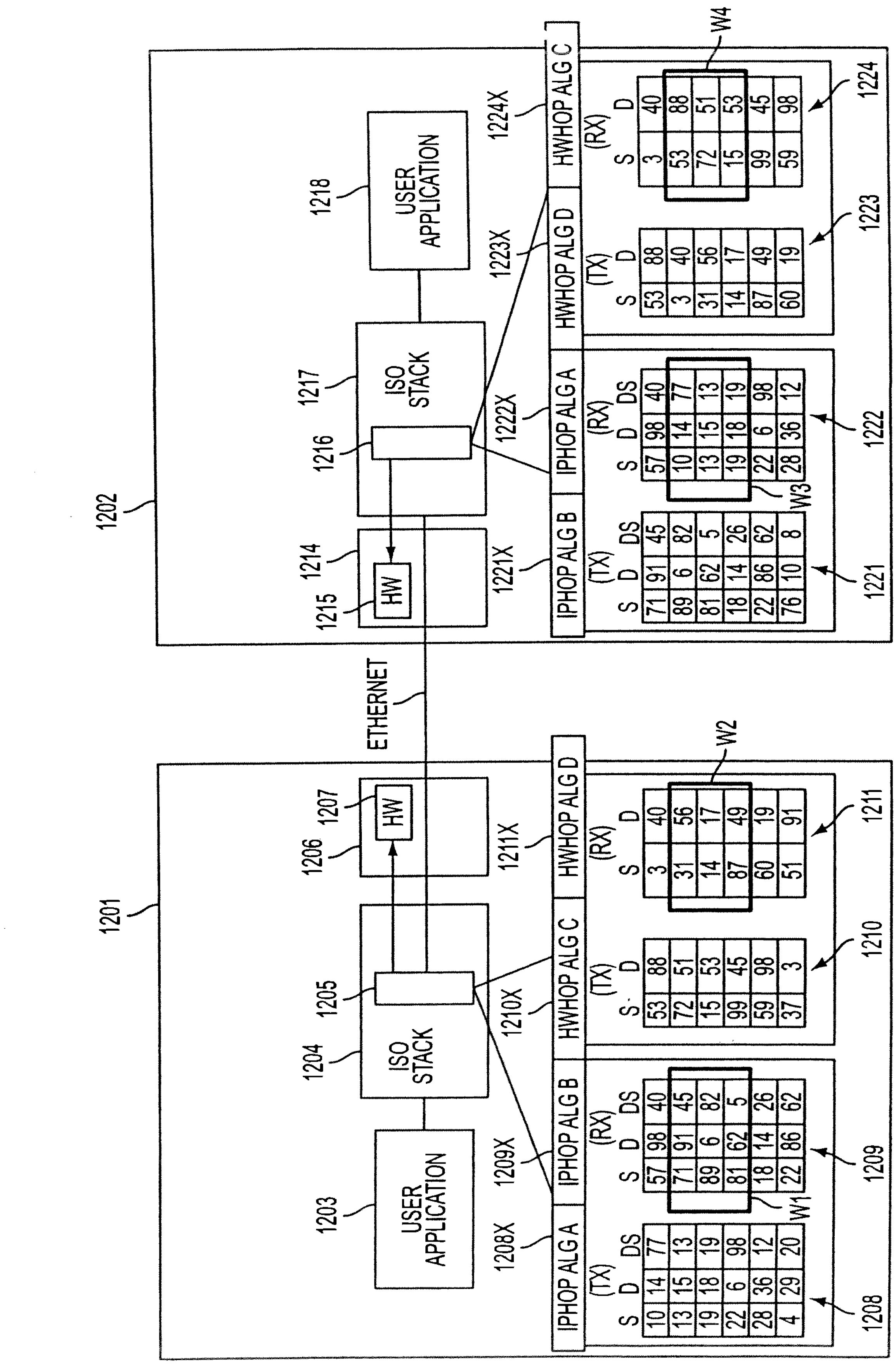

1201
1202
USER APPLICATION
ISO STACK
HW
ETHERNET
1203
1204
1205
1206
1207
1208X
1209X
1210X
1211X
IPHOP ALG A
IPHOP ALG B
HWHOP ALG C
HWHOP ALG D
(TX)
(RX)
1208
1209
1210
1211
W1
W2
1214
1215
1216
1217
1218
1221X
1222X
1223X
1224X
1221
1222
1223
1224
W3
W4

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

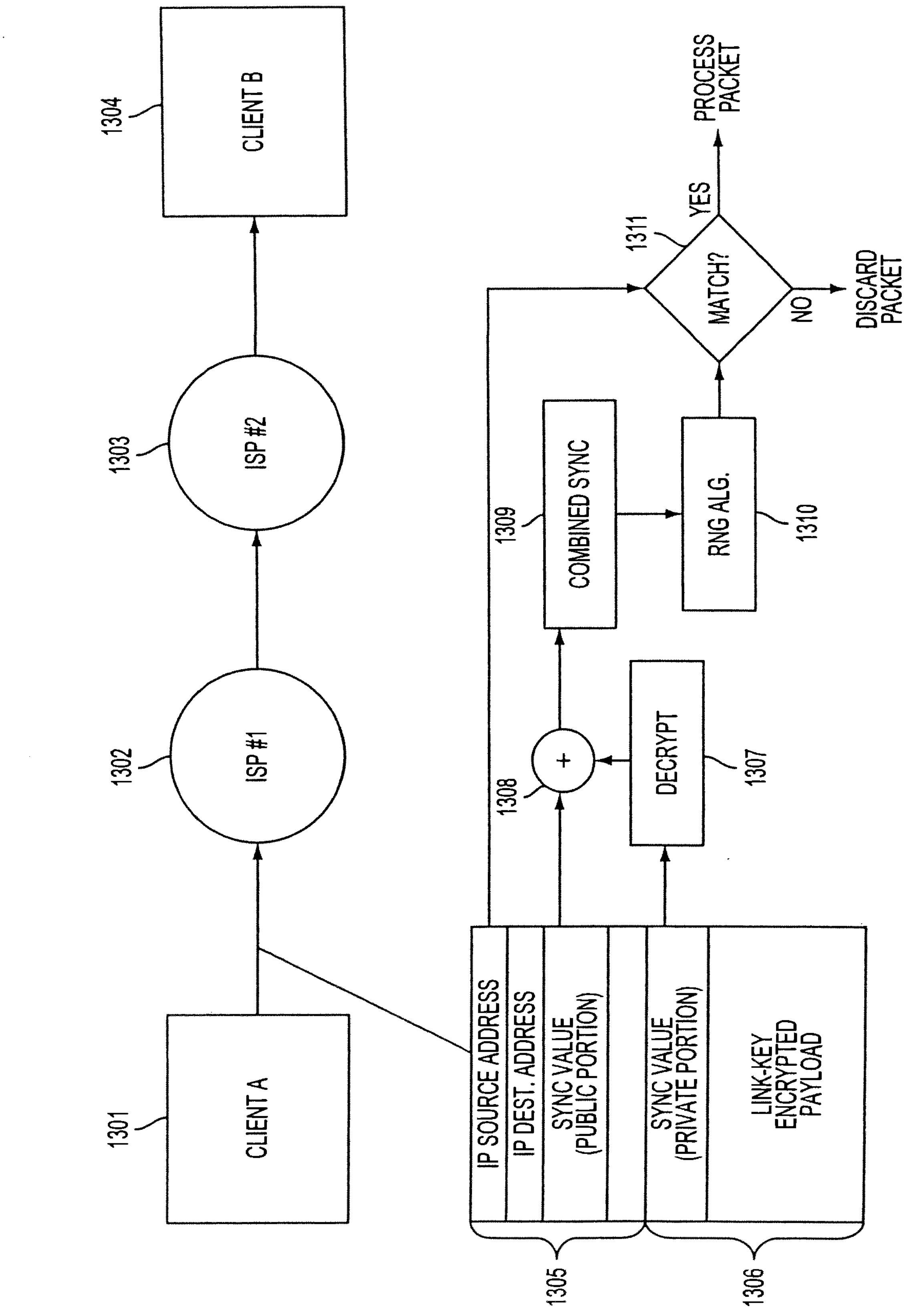

1301
CLIENT A
1302
ISP #1
1303
ISP #2
1304
CLIENT B
IP SOURCE ADDRESS
IP DEST. ADDRESS
SYNC VALUE (PUBLIC PORTION)
SYNC VALUE (PRIVATE PORTION)
LINK-KEY ENCRYPTED PAYLOAD
1305
1306
1307
DECRYPT
1308
+
1309
COMBINED SYNC
1310
RNG ALG.
1311
MATCH?
YES
NO
PROCESS PACKET
DISCARD PACKET

FIG. 13

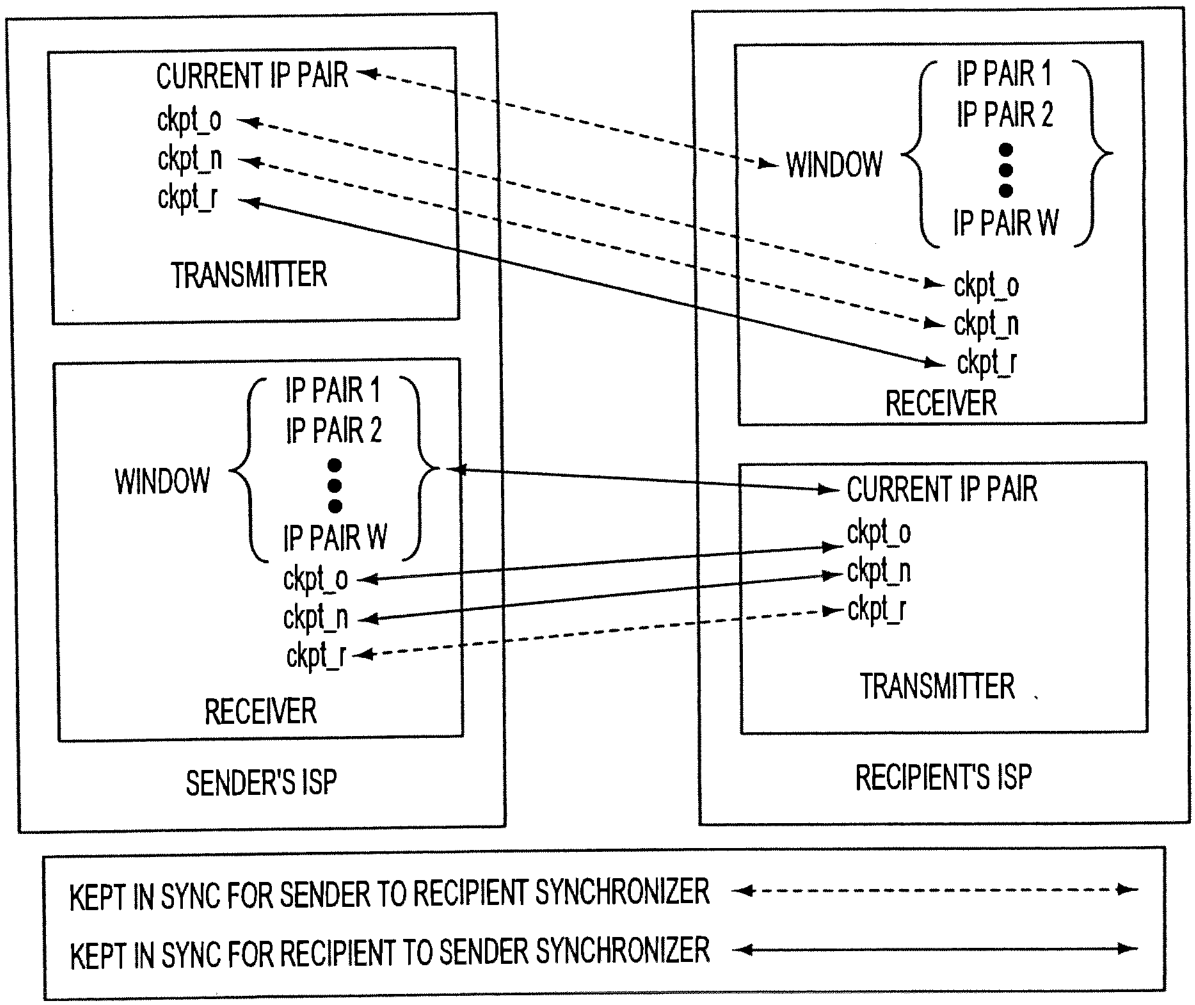

CURRENT IP PAIR
ckpt_o
ckpt_n
ckpt_r
TRANSMITTER
WINDOW
IP PAIR 1
IP PAIR 2
IP PAIR W
ckpt_o
ckpt_n
ckpt_r
RECEIVER
SENDER'S ISP
WINDOW
IP PAIR 1
IP PAIR 2
IP PAIR W
ckpt_o
ckpt_n
ckpt_r
RECEIVER
CURRENT IP PAIR
ckpt_o
ckpt_n
ckpt_r
TRANSMITTER
RECIPIENT'S ISP
KEPT IN SYNC FOR SENDER TO RECIPIENT SYNCHRONIZER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

FIG. 14

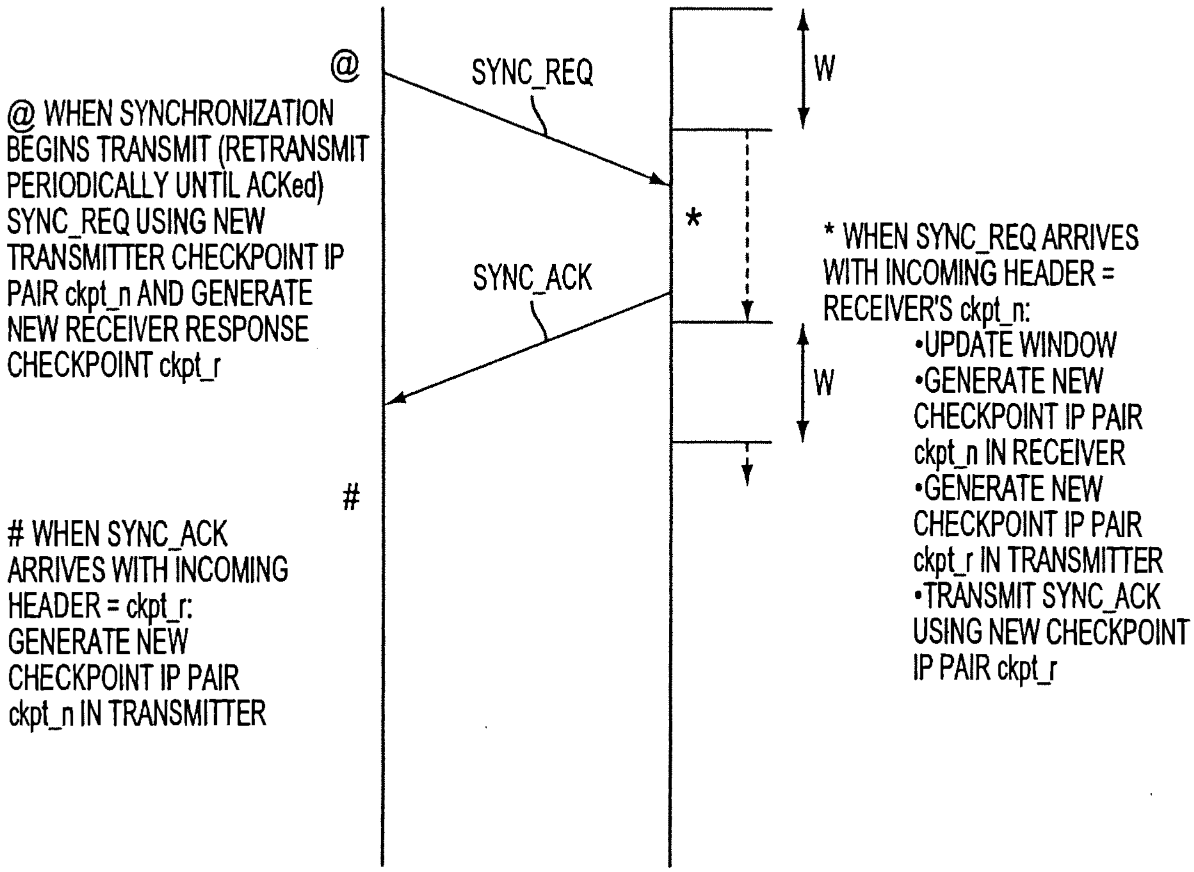

@
SYNC_REQ
W
@ WHEN SYNCHRONIZATION BEGINS TRANSMIT (RETRANSMIT PERIODICALLY UNTIL ACKed) SYNC_REQ USING NEW TRANSMITTER CHECKPOINT IP PAIR ckpt_n AND GENERATE NEW RECEIVER RESPONSE CHECKPOINT ckpt_r
*
* WHEN SYNC_REQ ARRIVES WITH INCOMING HEADER = RECEIVER'S ckpt_n:
•UPDATE WINDOW
•GENERATE NEW CHECKPOINT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

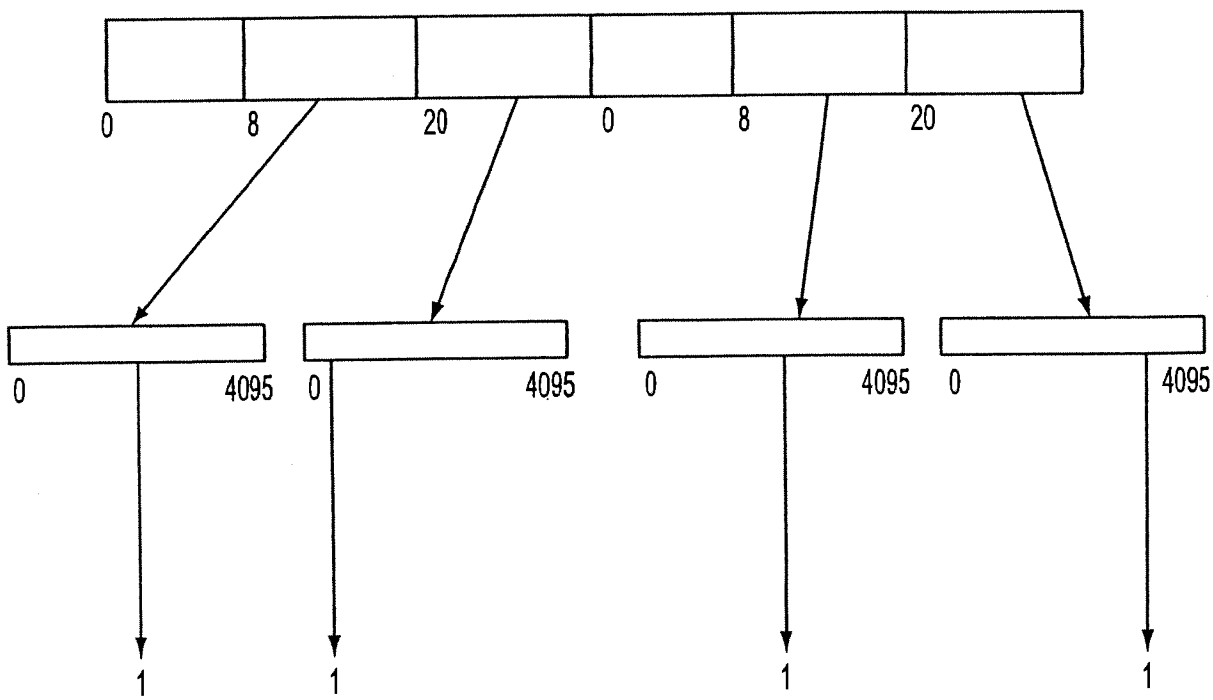


FIG. 16

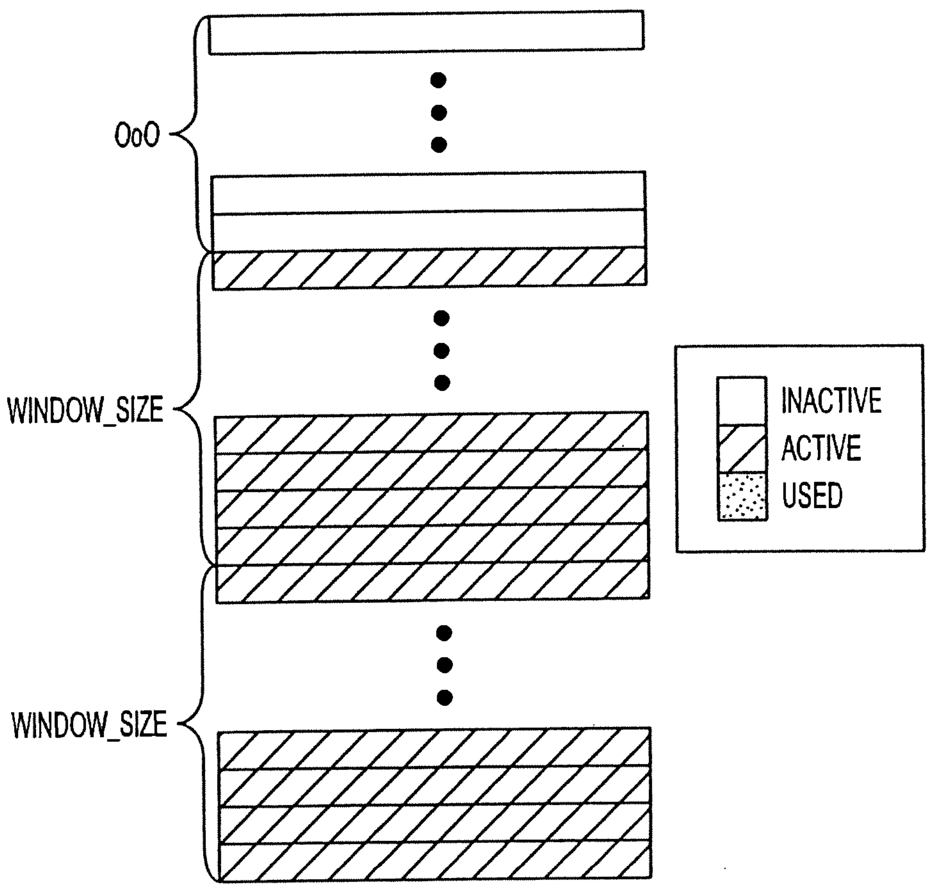


FIG. 17

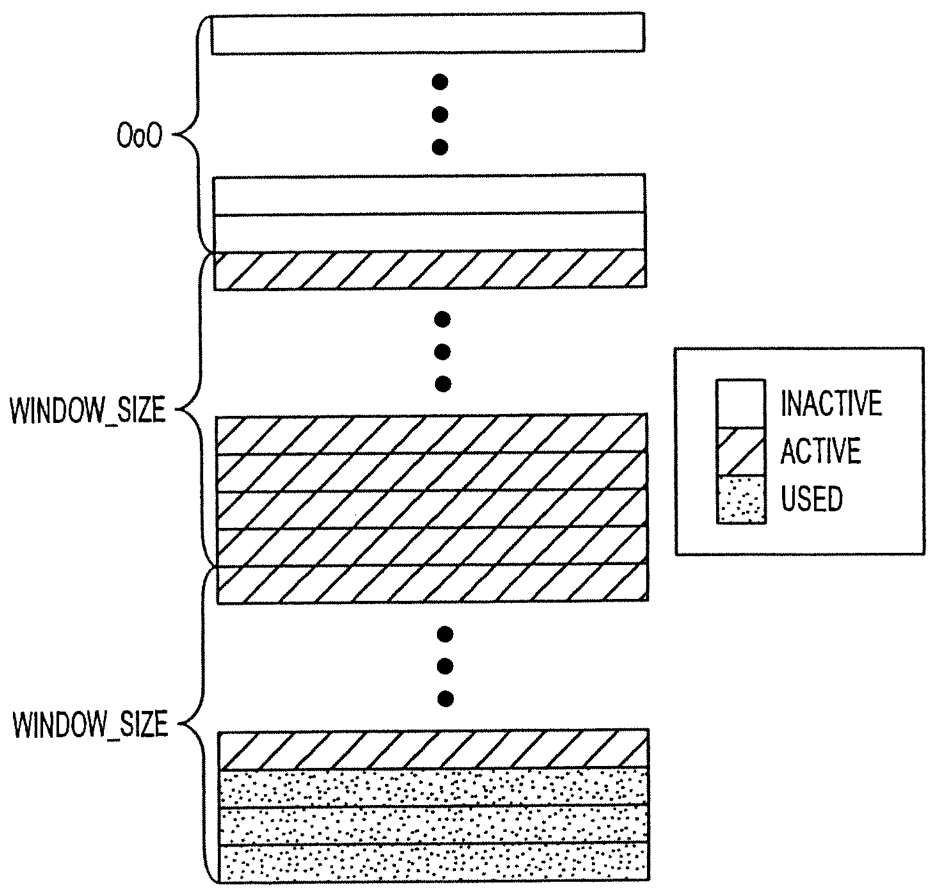


FIG. 18

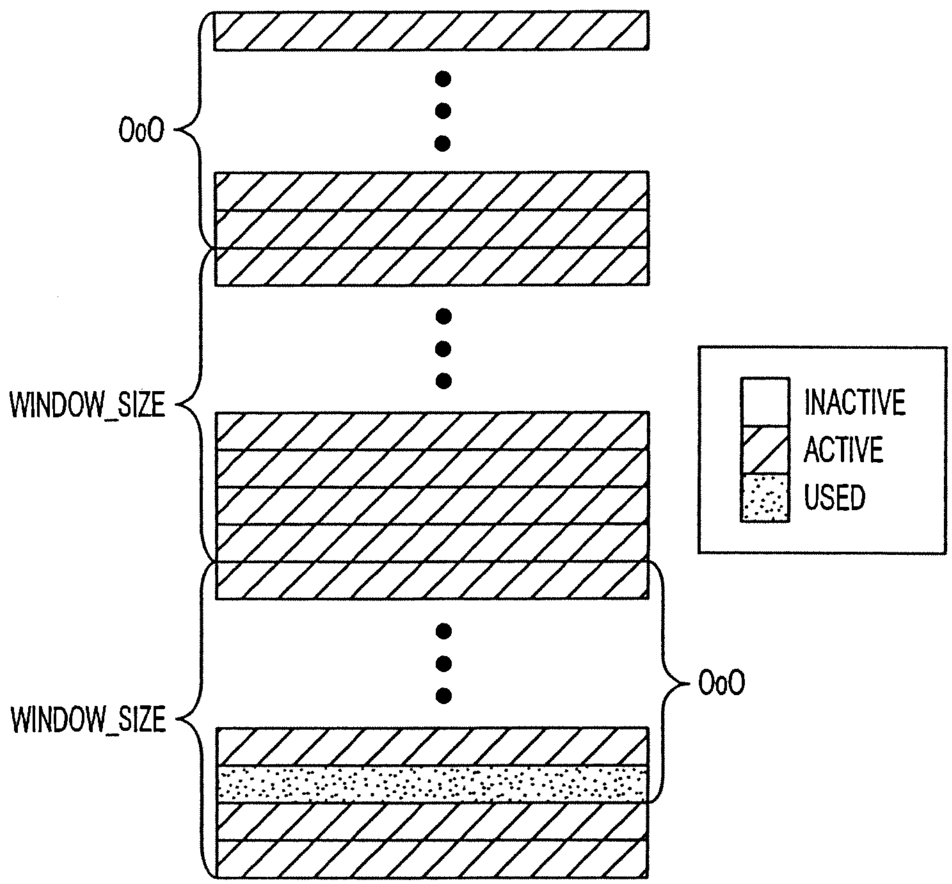


FIG. 19

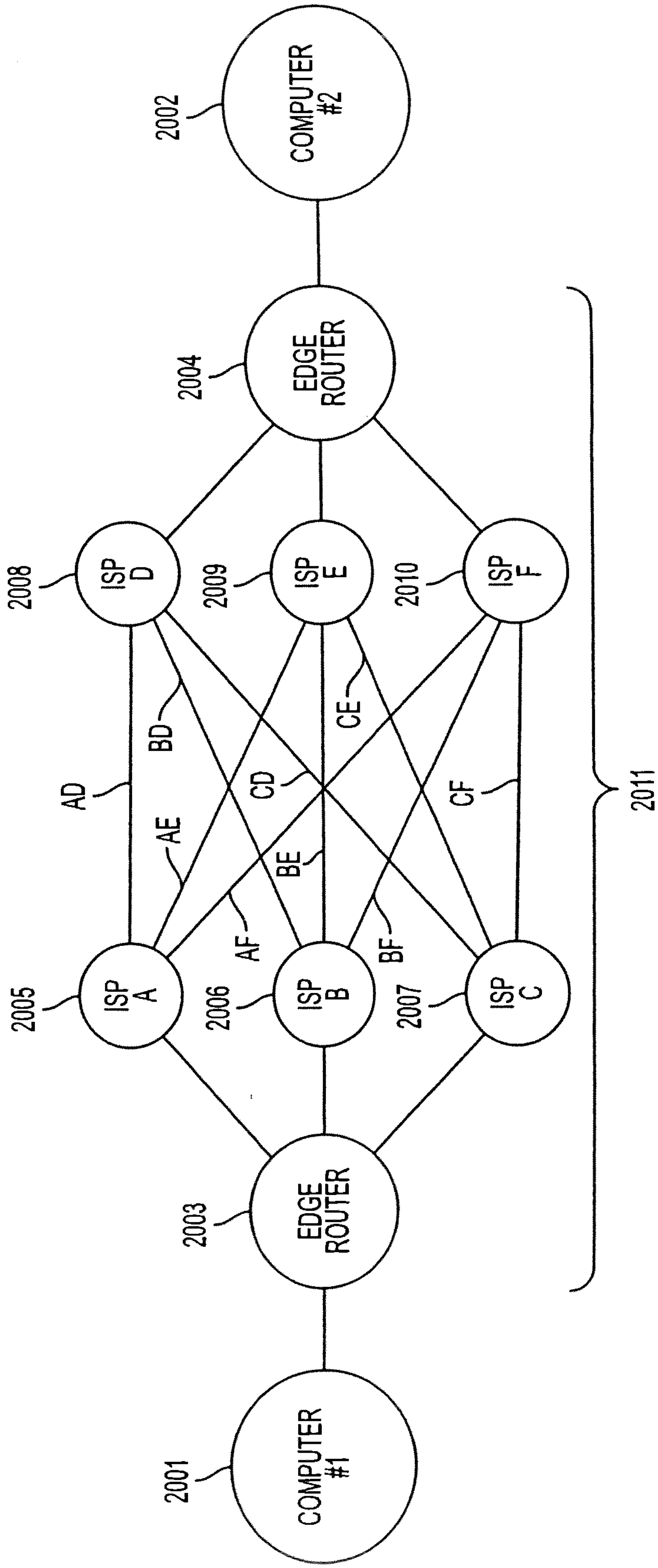

COMPUTER #1
2001
EDGE ROUTER
2003
ISP A
2005
ISP B
2006
ISP C
2007
ISP D
2008
ISP E
2009
ISP F
2010
EDGE ROUTER
2004
COMPUTER #2
2002
AD
AE
AF
BD
BE
BF
CD
CE
CF
2011

FIG. 20

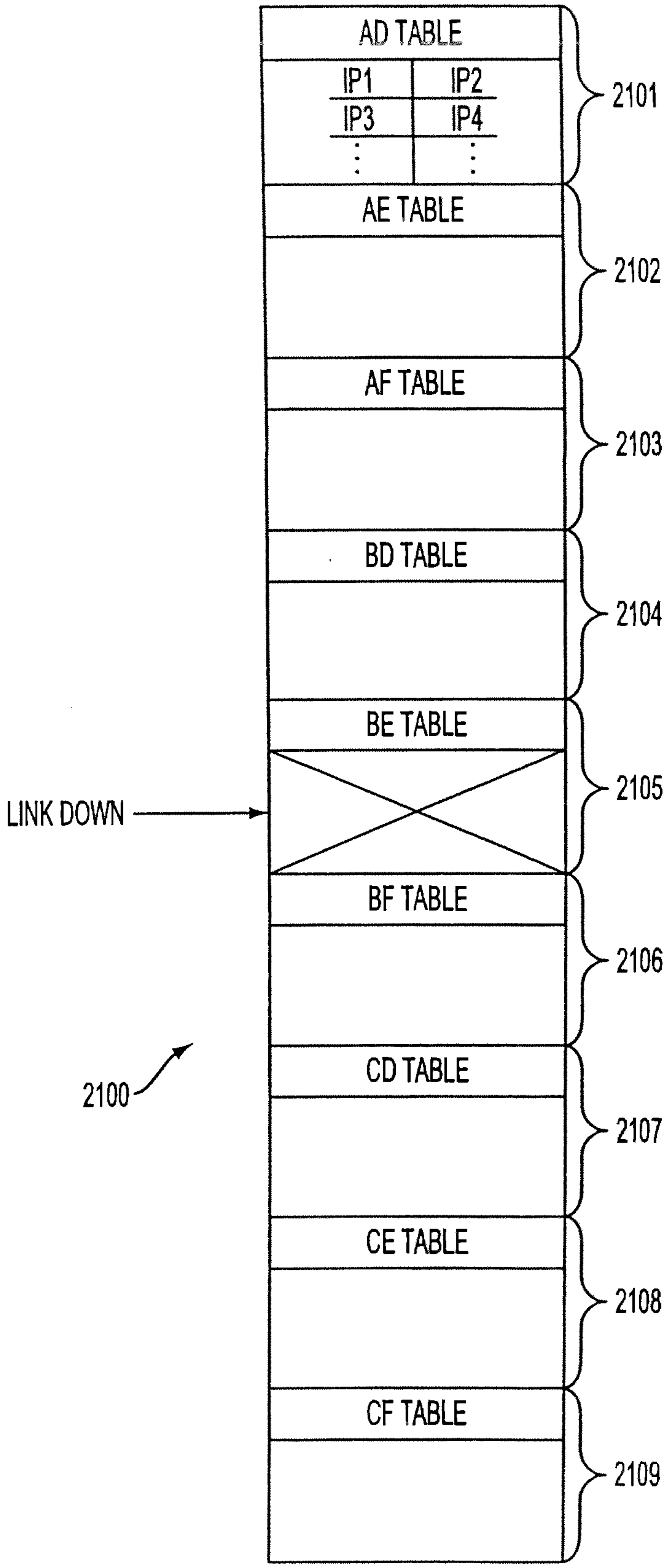
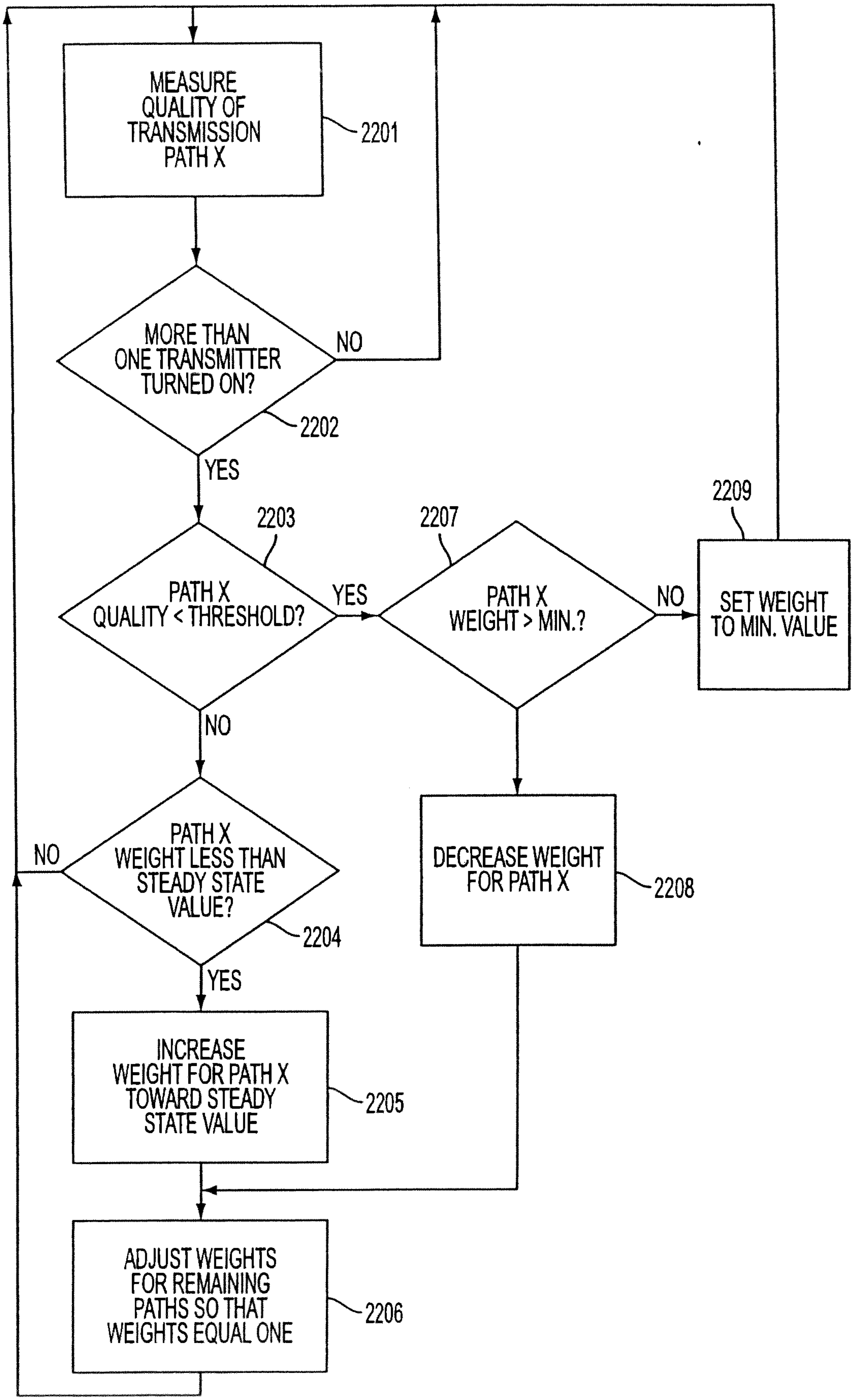

AD TABLE
IP1
IP2
IP3
IP4
2101
AE TABLE
2102
AF TABLE
2103
BD TABLE
2104
BE TABLE
LINK DOWN
2105
BF TABLE
2106
2100
CD TABLE
2107
CE TABLE
2108
CF TABLE
2109

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

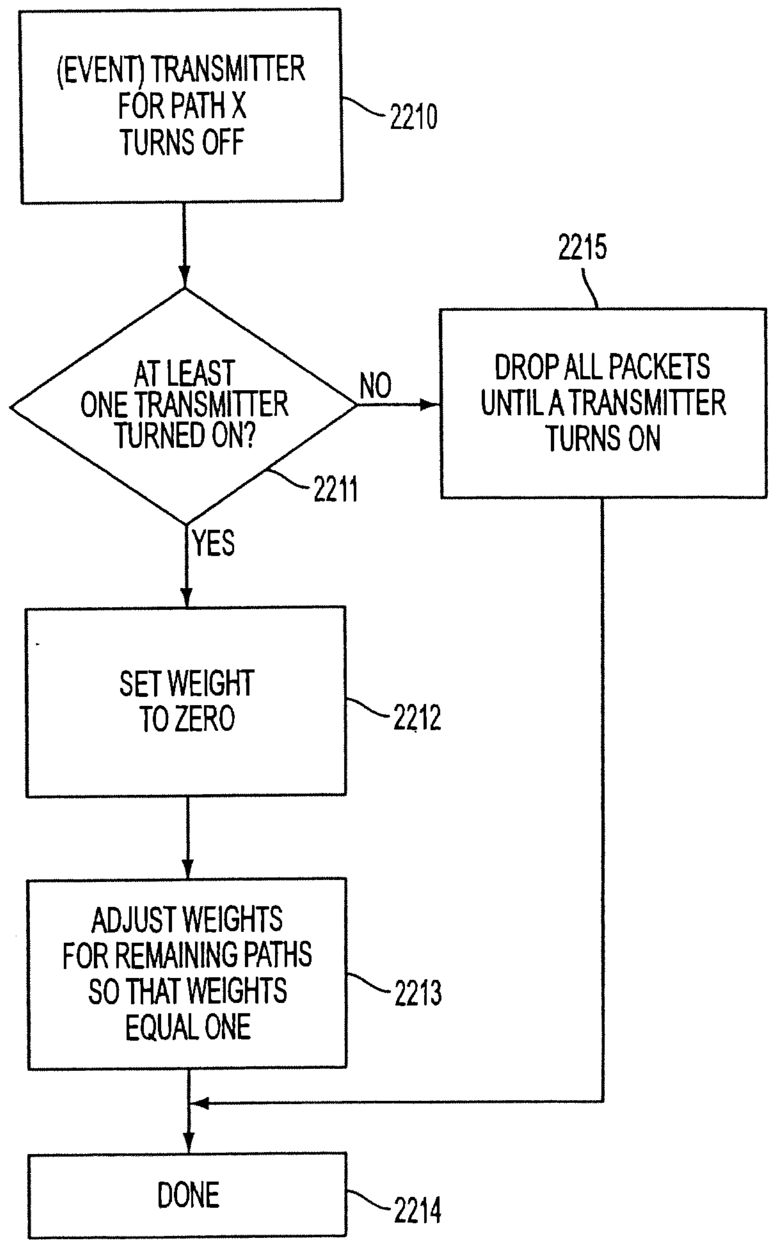

(EVENT) TRANSMITTER FOR PATH X TURNS OFF
2210
2215
AT LEAST ONE TRANSMITTER TURNED ON?
NO
DROP ALL PACKETS UNTIL A TRANSMITTER TURNS ON
2211
YES
SET WEIGHT TO ZERO
2212
ADJUST WEIGHTS FOR REMAINING PATHS SO THAT WEIGHTS EQUAL ONE
2213
DONE
2214

FIG. 22B

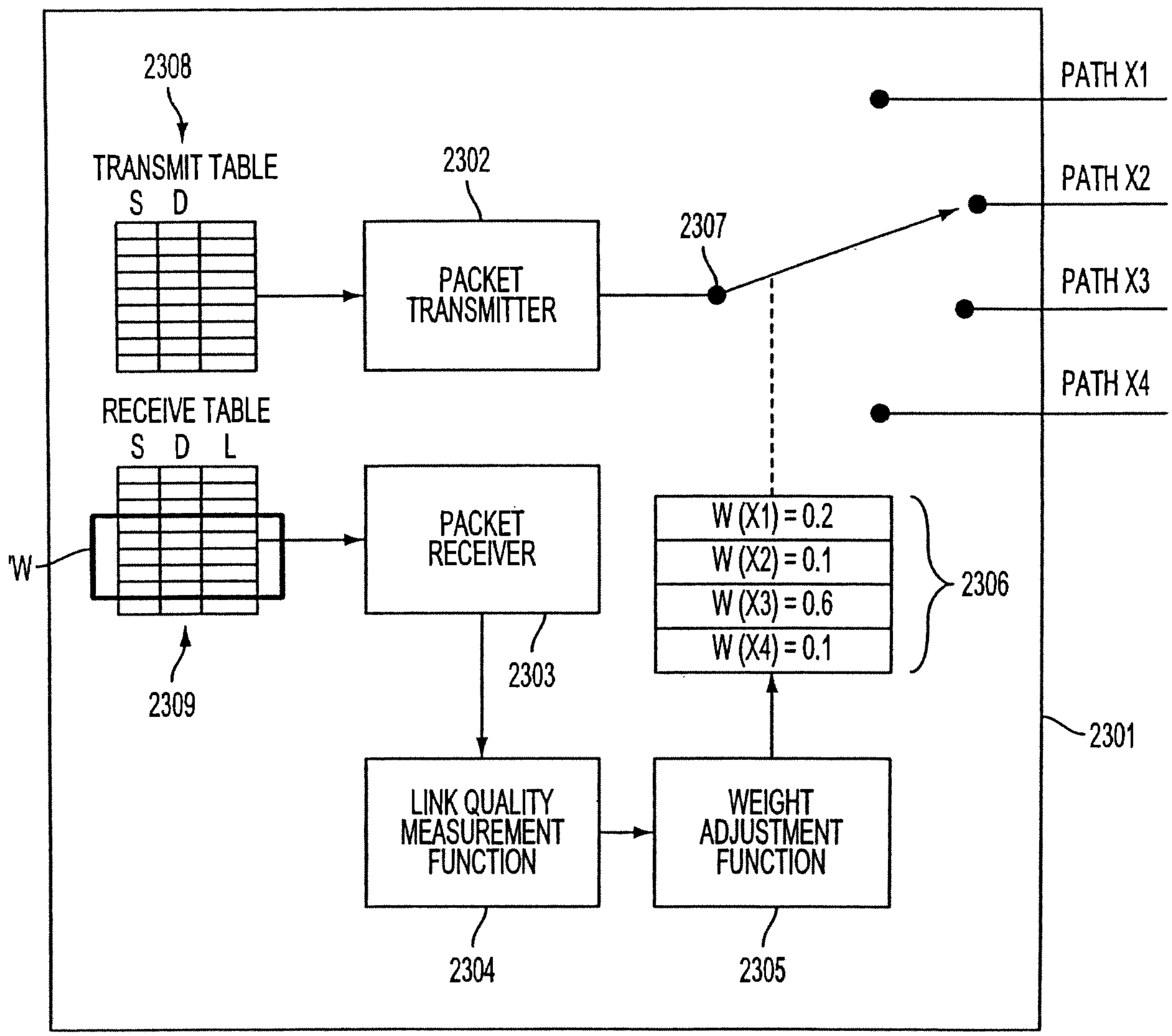

2308
TRANSMIT TABLE
S D
2302
PACKET TRANSMITTER
2307
PATH X1
PATH X2
PATH X3
PATH X4
RECEIVE TABLE
S D L
W
PACKET RECEIVER
W (X1) = 0.2
W (X2) = 0.1
W (X3) = 0.6
W (X4) = 0.1
2306
2309
2303
2301
LINK QUALITY MEASUREMENT FUNCTION
WEIGHT ADJUSTMENT FUNCTION
2304
2305

FIG. 23

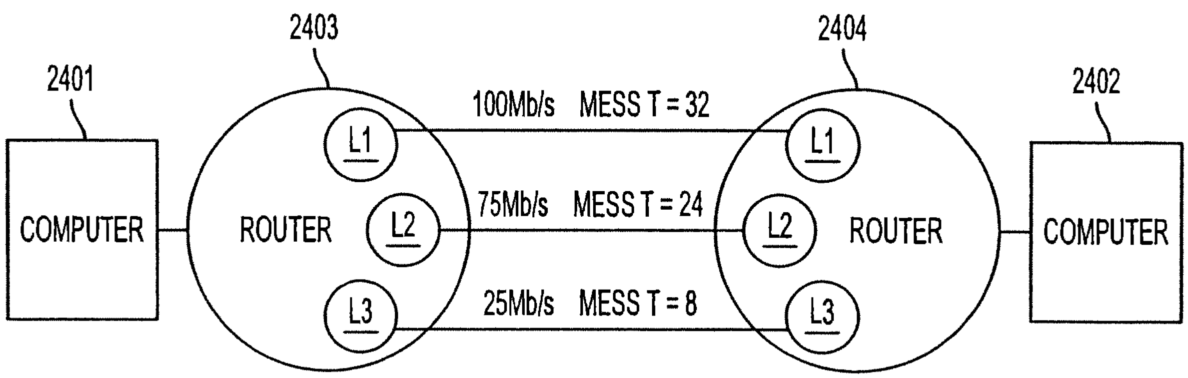

2401
2403
2404
2402
COMPUTER
ROUTER
L1
L2
L3
100Mb/s MESS T = 32
75Mb/s MESS T = 24
25Mb/s MESS T = 8
L1
L2
L3
ROUTER
COMPUTER

FIG. 24

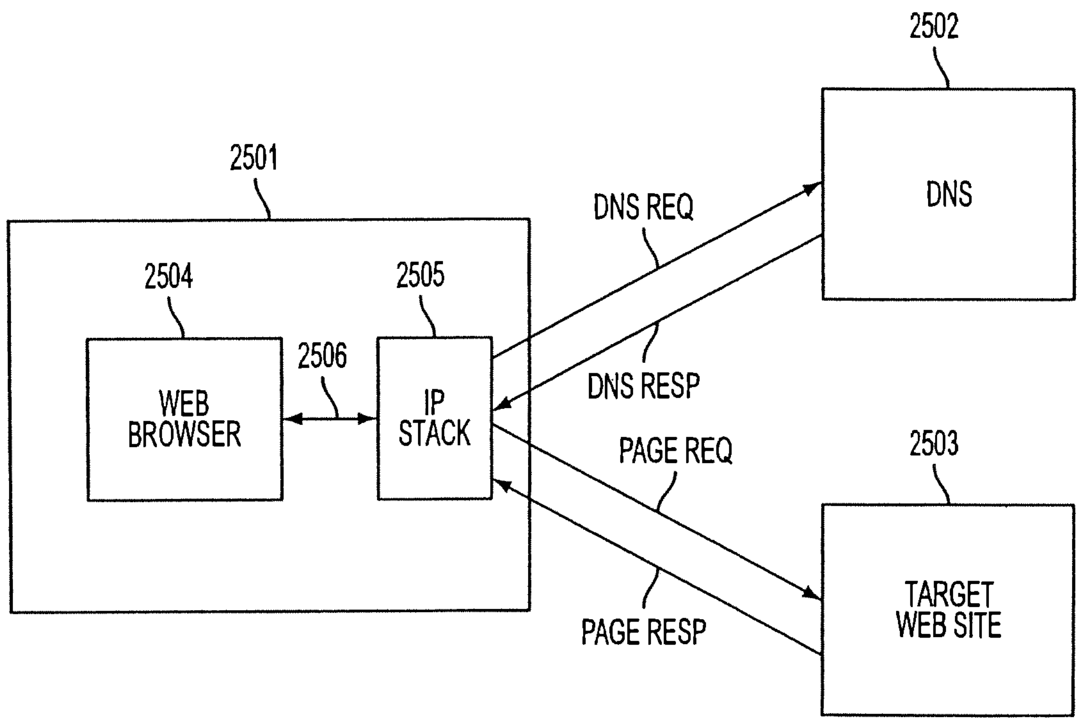


FIG. 25
(PRIOR ART)

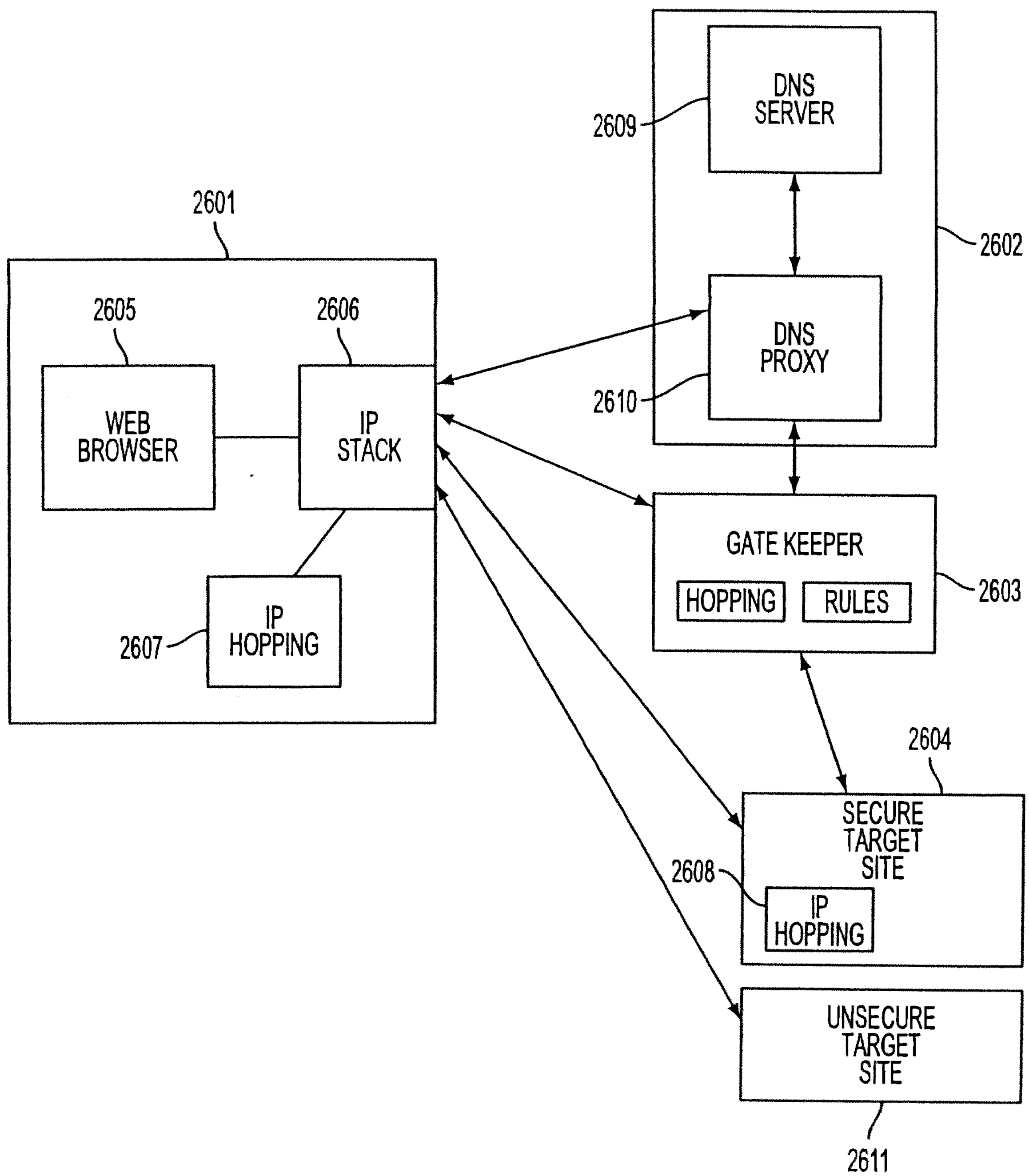

2601
2605
2606
WEB BROWSER
IP STACK
IP HOPPING
2607
2609
DNS SERVER
2602
DNS PROXY
2610
GATE KEEPER
HOPPING
RULES
2603
2604
SECURE TARGET SITE
2608
IP HOPPING
UNSECURE TARGET SITE
2611

FIG. 26

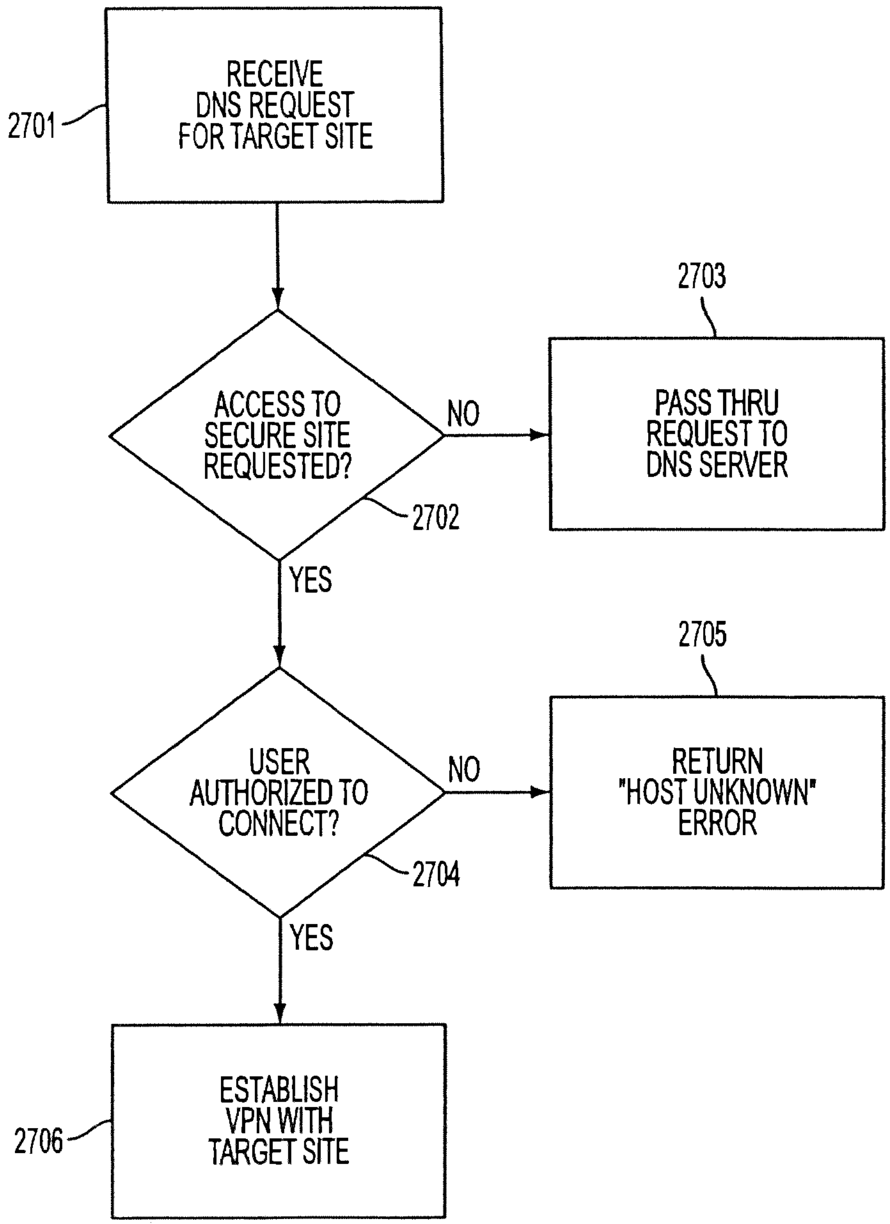

RECEIVE DNS REQUEST FOR TARGET SITE
2701
ACCESS TO SECURE SITE REQUESTED?
2702
NO
PASS THRU REQUEST TO DNS SERVER
2703
YES
USER AUTHORIZED TO CONNECT?
2704
NO
RETURN "HOST UNKNOWN" ERROR
2705
YES
ESTABLISH VPN WITH TARGET SITE
2706

FIG. 27

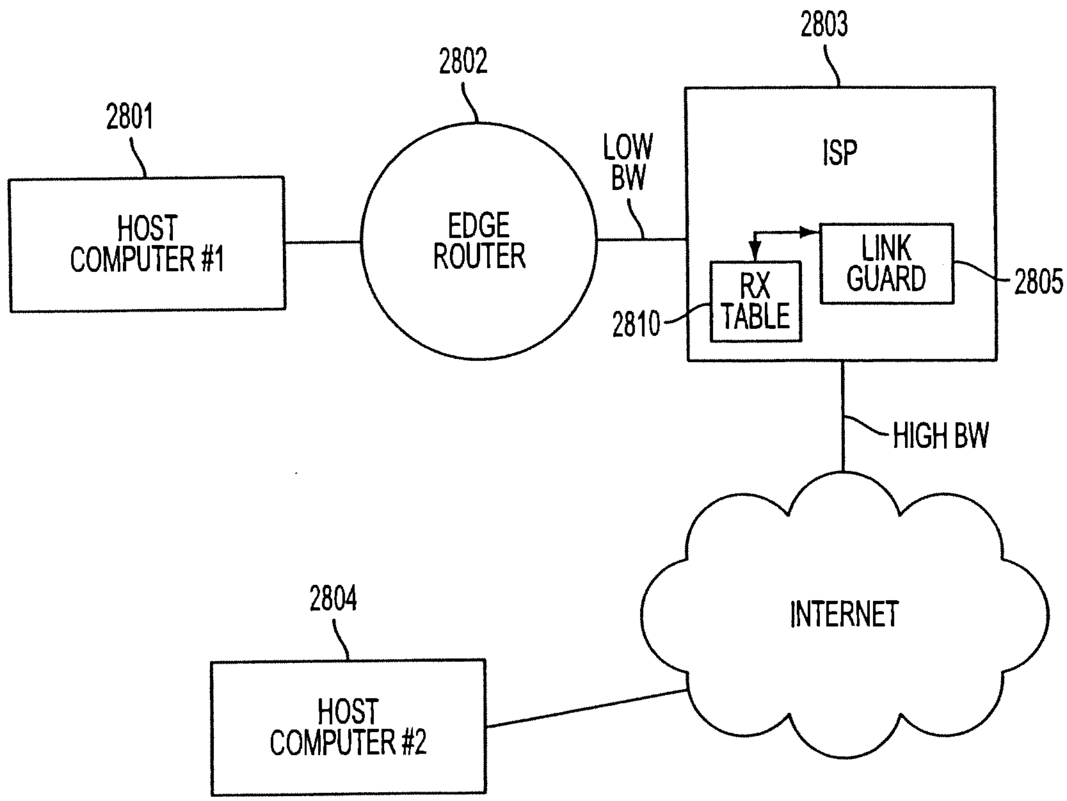

2801
HOST COMPUTER #1
2802
EDGE ROUTER
LOW BW
2803
ISP
LINK GUARD
2805
RX TABLE
2810
HIGH BW
INTERNET
2804
HOST COMPUTER #2

FIG. 28

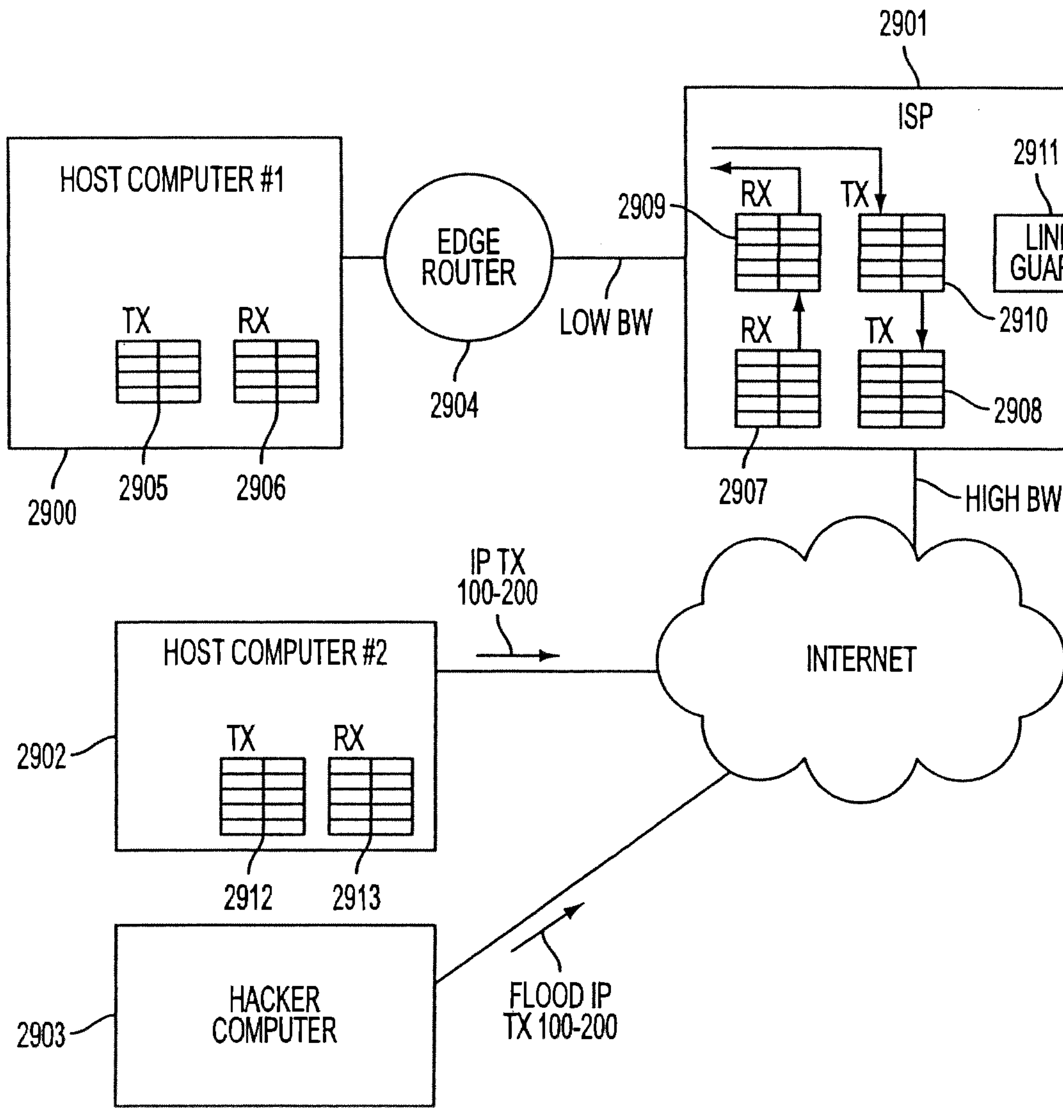
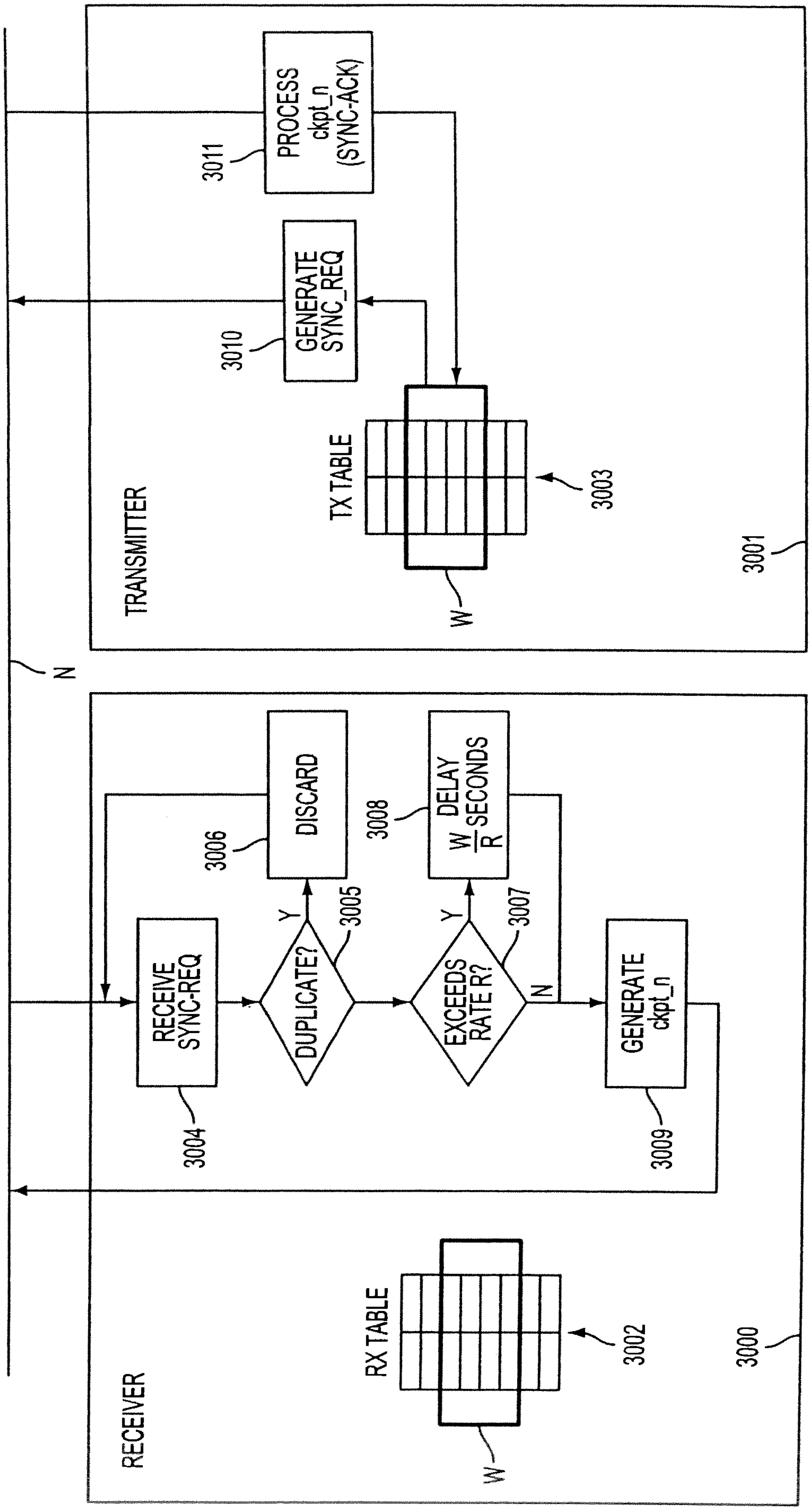

2901
ISP
2911
LINK GUARD
HOST COMPUTER #1
EDGE ROUTER
2909
RX
TX
2910
RX
TX
2908
LOW BW
2904
TX
RX
2900
2905
2906
2907
HIGH BW
IP TX 100-200
HOST COMPUTER #2
INTERNET
2902
TX
RX
2912
2913
HACKER COMPUTER
2903
FLOOD IP TX 100-200

FIG. 29



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

FIG. 30

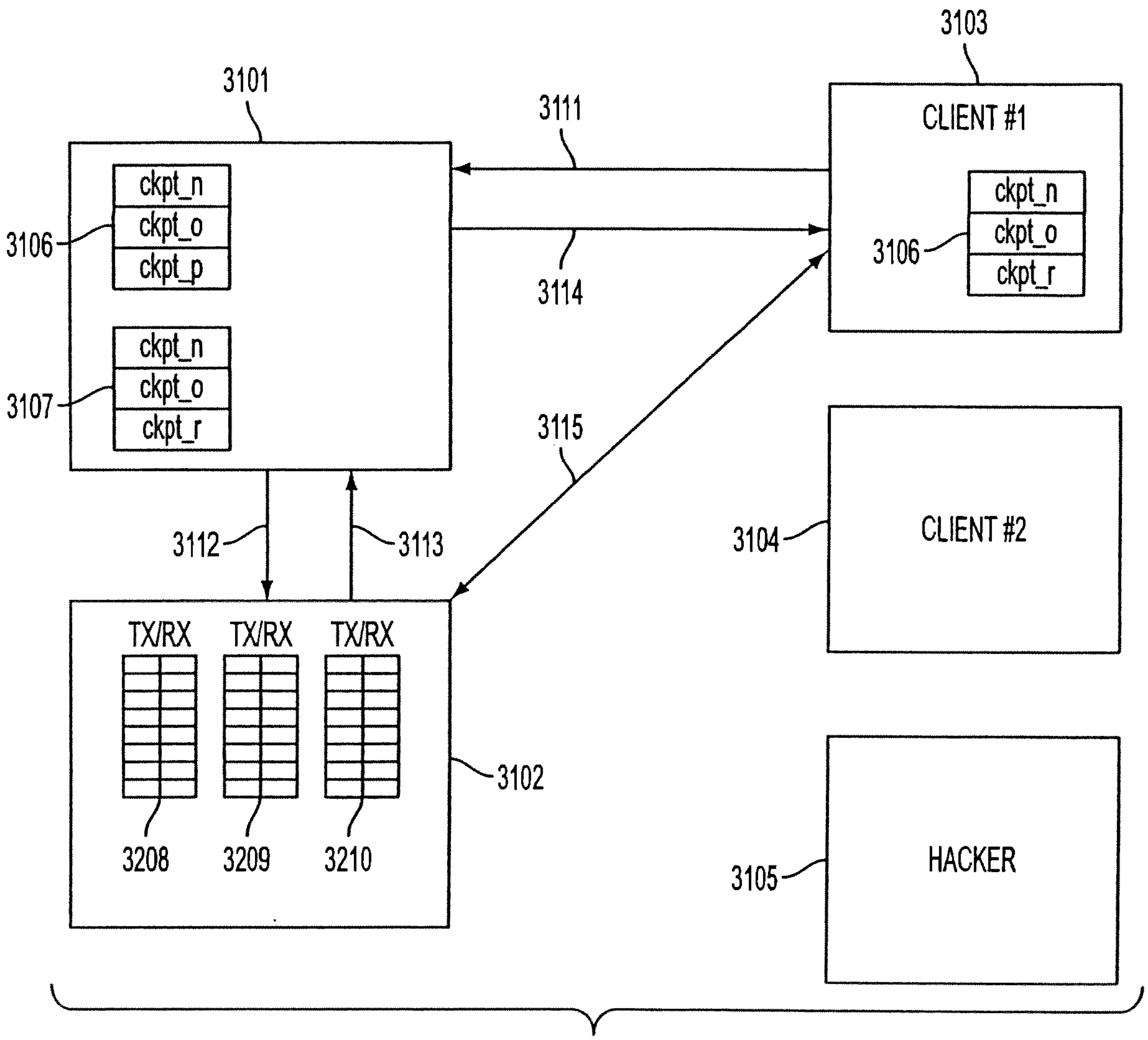

3103
3101
3111
CLIENT #1
ckpt_n
ckpt_o
ckpt_p
3106
ckpt_n
ckpt_o
ckpt_r
3106
3114
ckpt_n
ckpt_o
ckpt_r
3107
3115
CLIENT #2
3104
3112
3113
TX/RX
TX/RX
TX/RX
3102
3208
3209
3210
HACKER
3105

FIG. 31

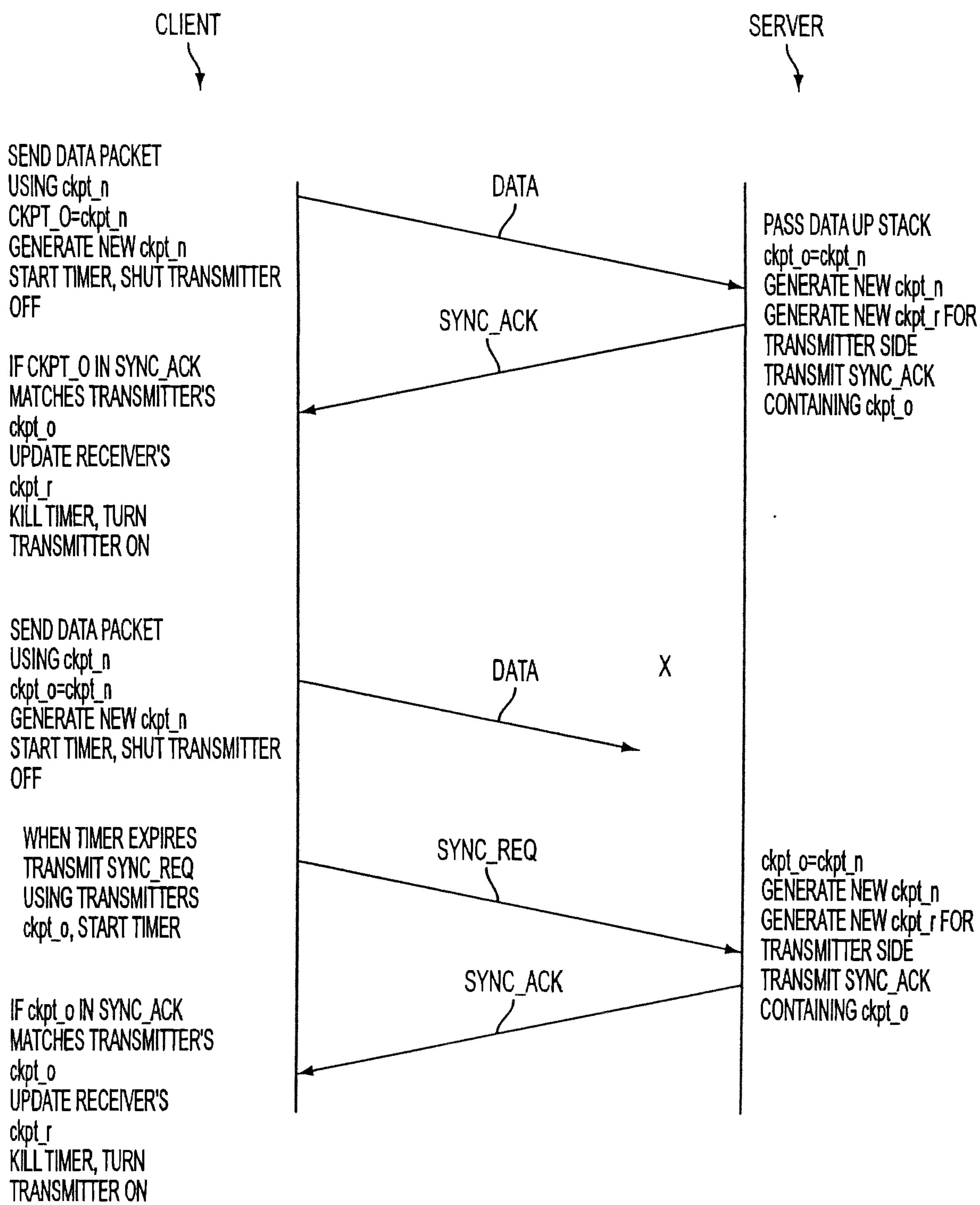

CLIENT
SERVER
SEND DATA PACKET
USING ckpt_n
CKPT_O=ckpt_n
GENERATE NEW ckpt_n
START TIMER, SHUT TRANSMITTER
OFF
DATA
PASS DATA UP STACK
ckpt_o=ckpt_n
GENERATE NEW ckpt_n
GENERATE NEW ckpt_r FOR
TRANSMITTER SIDE
TRANSMIT SYNC_ACK
CONTAINING ckpt_o
SYNC_ACK
IF CKPT_O IN SYNC_ACK
MATCHES TRANSMITTER'S
ckpt_o
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

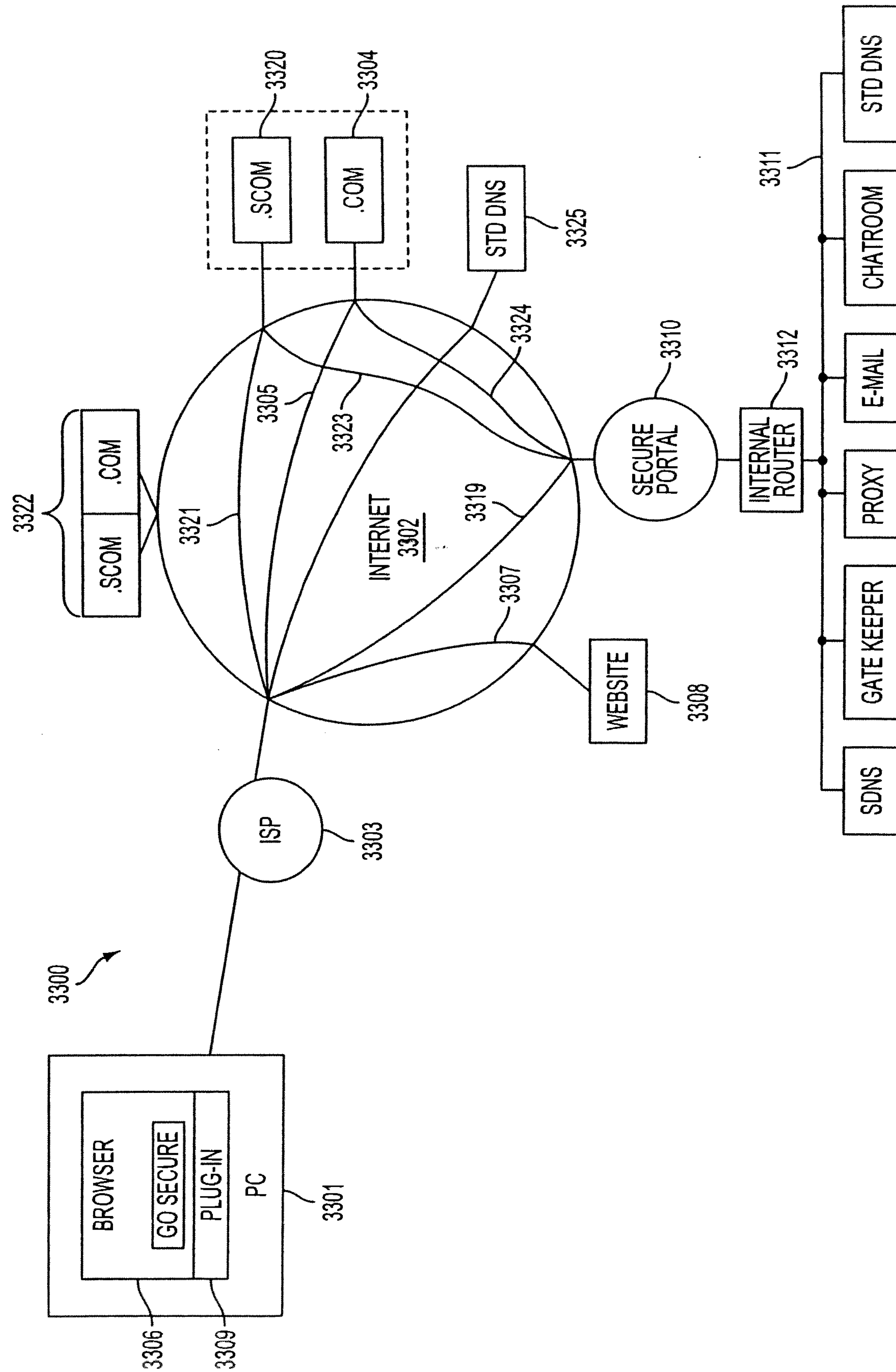
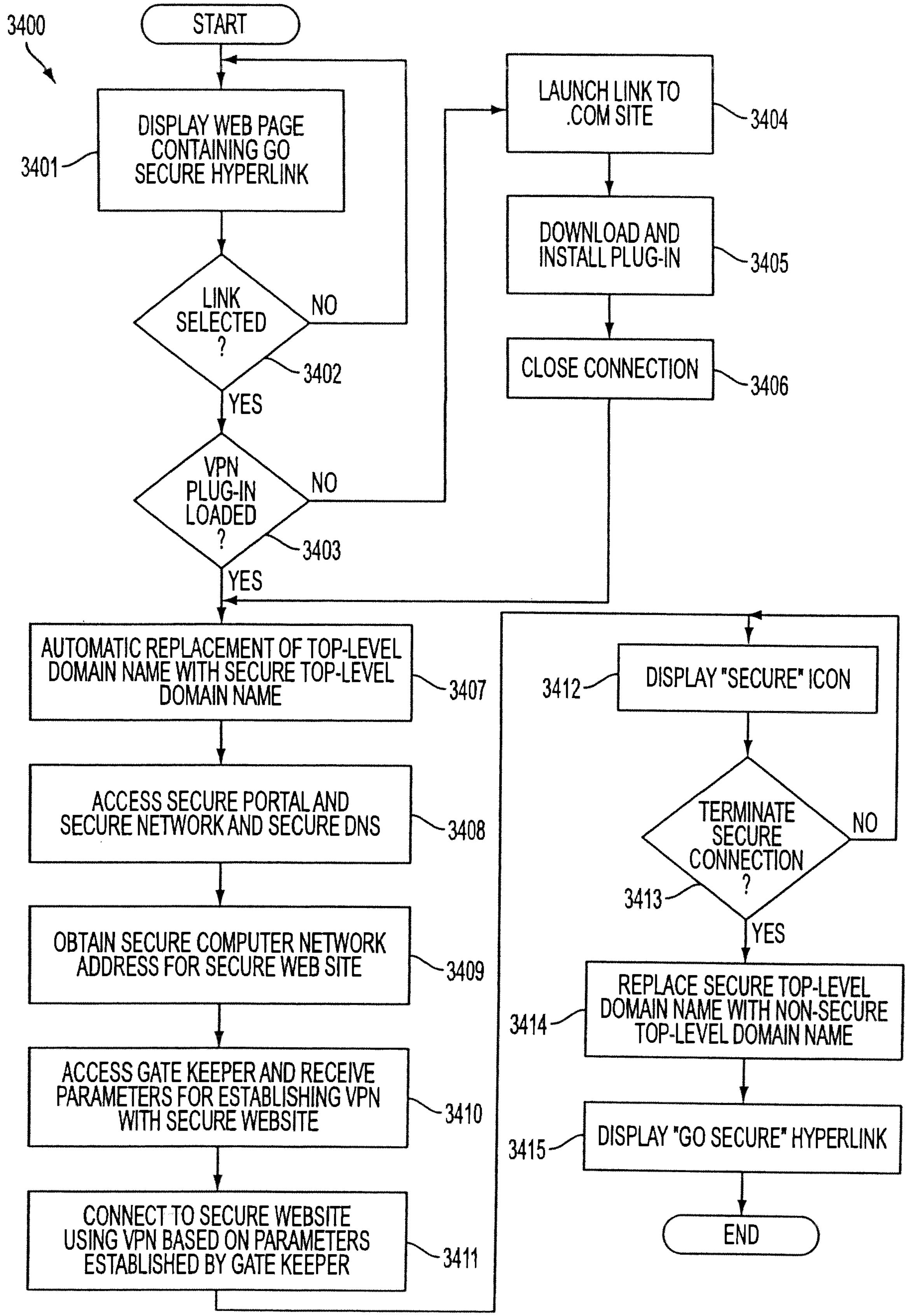

3300
PC
BROWSER
GO SECURE
PLUG-IN
3301
3306
3309
ISP
3303
INTERNET
3302
3321
3305
3323
3324
3319
3307
3322
.SCOM
.COM
3320
3304
STD DNS
3325
WEBSITE
3308
SECURE PORTAL
3310
INTERNAL ROUTER
3312
3311
SDNS
3313
GATE KEEPER
3314
PROXY
3315
E-MAIL
3316
CHATROOM
3317
STD DNS
3318

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
DISPLAY "SECURE" ICON
3412
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

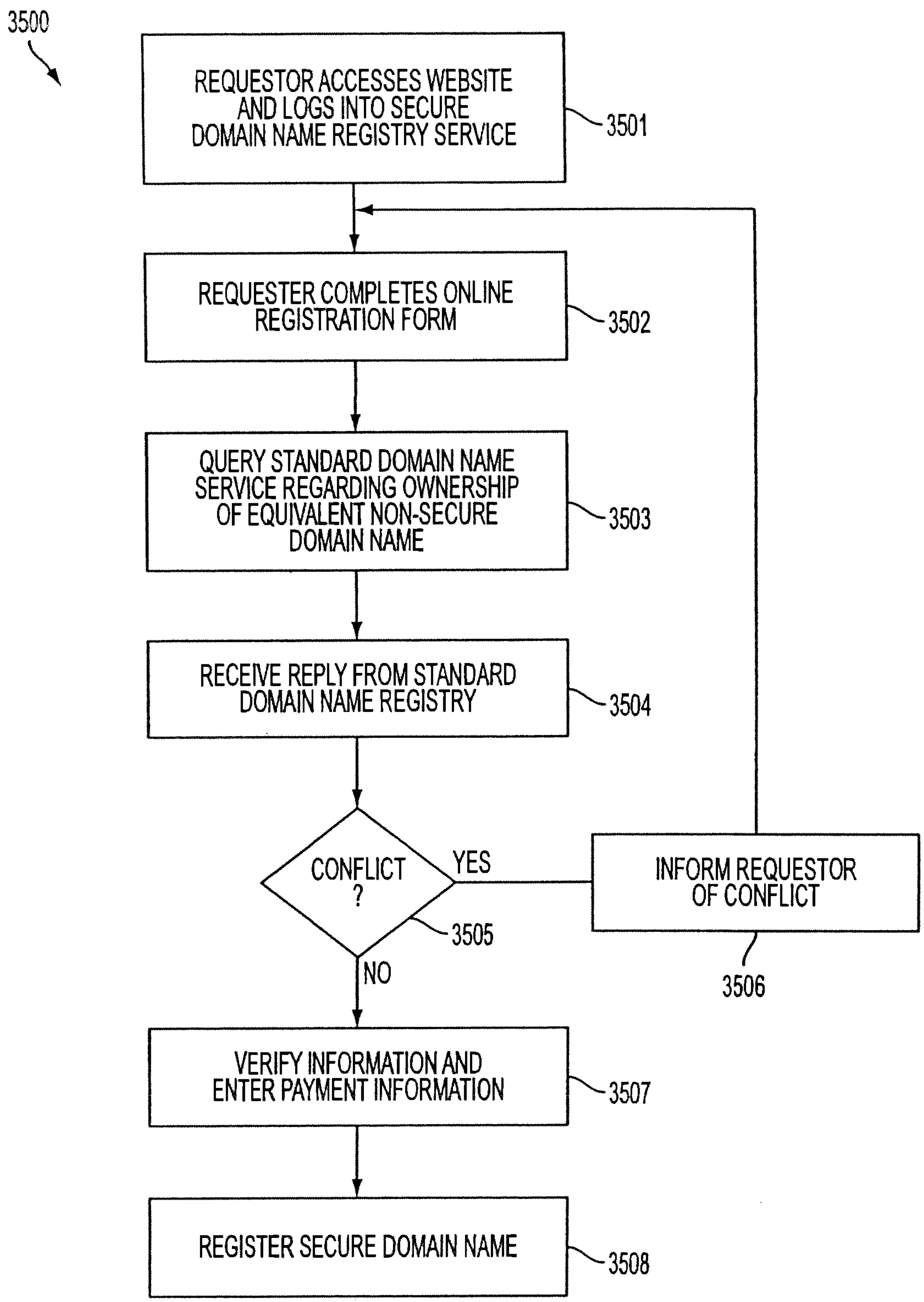

3500
REQUESTOR ACCESSES WEBSITE AND LOGS INTO SECURE DOMAIN NAME REGISTRY SERVICE
3501
REQUESTER COMPLETES ONLINE REGISTRATION FORM
3502
QUERY STANDARD DOMAIN NAME SERVICE REGARDING OWNERSHIP OF EQUIVALENT NON-SECURE DOMAIN NAME
3503
RECEIVE REPLY FROM STANDARD DOMAIN NAME REGISTRY
3504
CONFLICT ?
3505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

FIG. 35

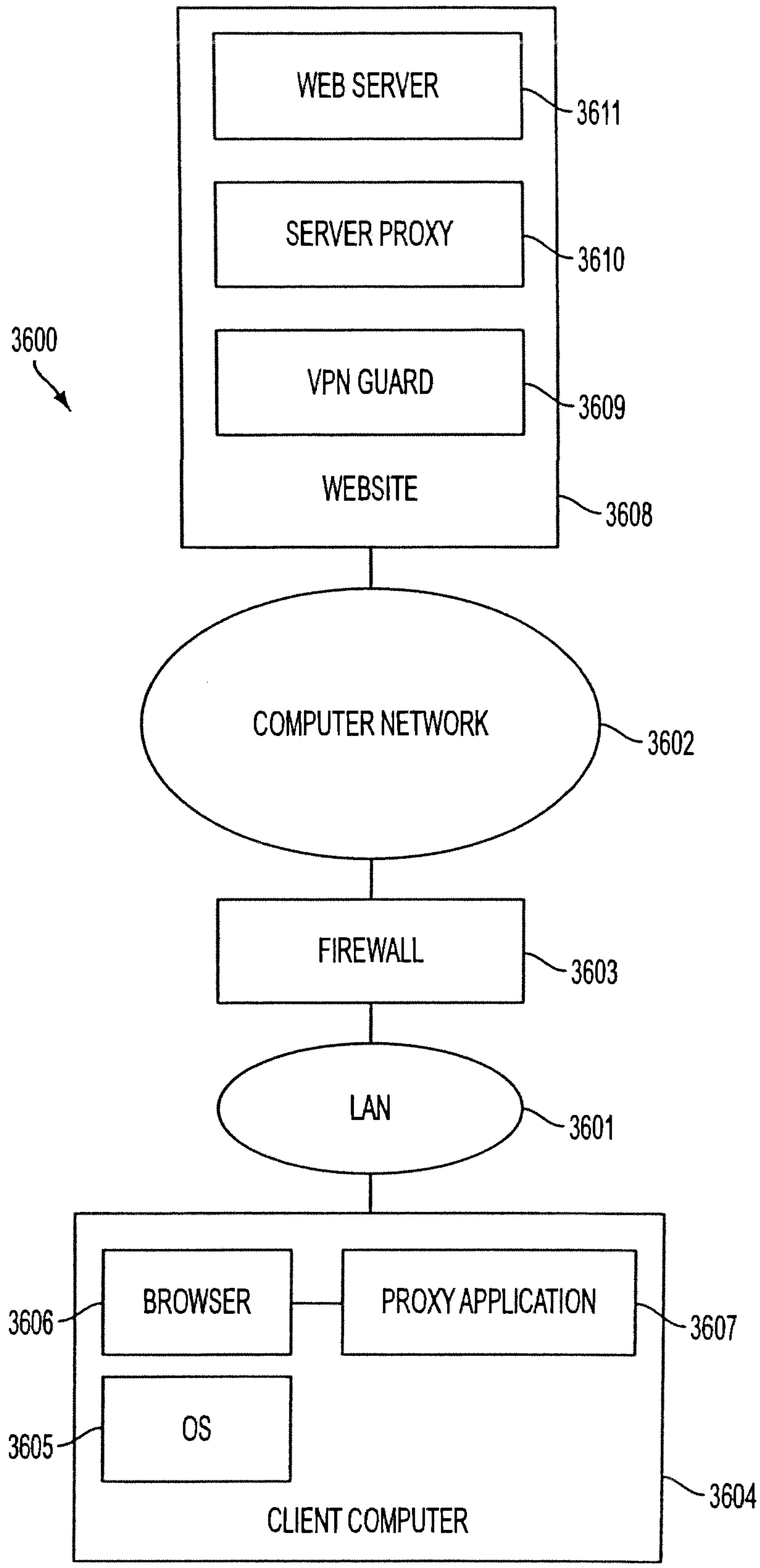

WEB SERVER
3611
SERVER PROXY
3610
3600
VPN GUARD
3609
WEBSITE
3608
COMPUTER NETWORK
3602
FIREWALL
3603
LAN
3601
BROWSER
3606
PROXY APPLICATION
3607
OS
3605
3604
CLIENT COMPUTER

FIG. 36

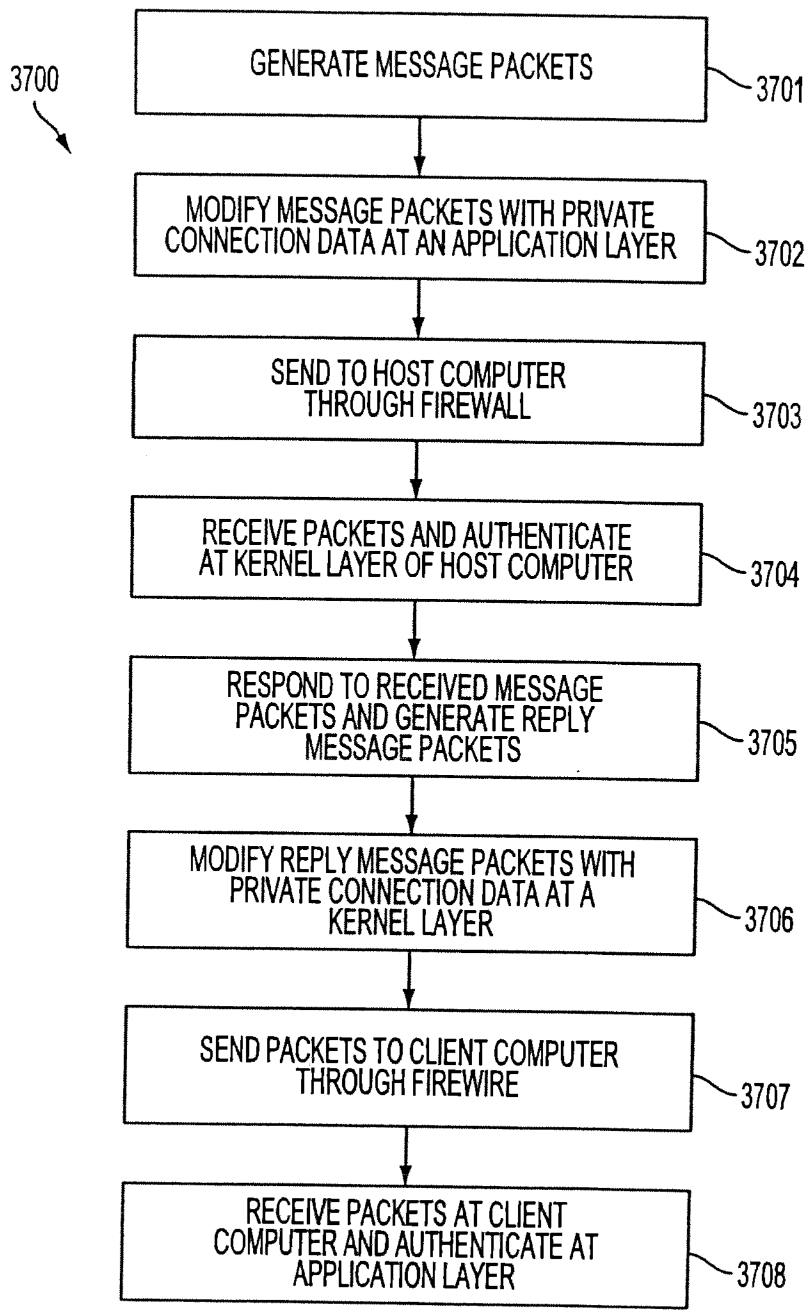

3700
GENERATE MESSAGE PACKETS
3701
MODIFY MESSAGE PACKETS WITH PRIVATE CONNECTION DATA AT AN APPLICATION LAYER
3702
SEND TO HOST COMPUTER THROUGH FIREWALL
3703
RECEIVE PACKETS AND AUTHENTICATE AT KERNEL LAYER OF HOST COMPUTER
3704
RESPOND TO RECEIVED MESSAGE PACKETS AND GENERATE REPLY MESSAGE PACKETS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

Electronic Acknowledgement Receipt

EFS ID:	14292943
Application Number:	13615557
International Application Number:	
Confirmation Number:	1089
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kimila Carraway
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	077580-0177
Receipt Date:	21-NOV-2012
Filing Date:	13-SEP-2012
Time Stamp:	21:11:40
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		077580-0177_Response_Notice_File_Corrected_Application_Papers.pdf	3302771 7c1dce8a42dd3a150c16fa4a4182bb7bb646c7b0	yes	42

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Applicant Response to Pre-Exam Formalities Notice	1	1
	Abstract	2	2
	Drawings-only black and white line drawings	3	42
Warnings:			
Information:			
	Total Files Size (in bytes):	3302771	

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
13/615,557

APPLICATION AS FILED - PART I

FOR	NUMBER FILED (Column 1)	NUMBER EXTRA (Column 2)	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	390
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))	20 minus 20 =	*			OR	x 62 =	0.00
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
			TOTAL			TOTAL	1260

* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED - PART II

AMENDMENT A

	CLAIMS REMAINING AFTER AMENDMENT (Column 1)		HIGHEST NUMBER PREVIOUSLY PAID FOR (Column 2)	PRESENT EXTRA (Column 3)	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))	*	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	

AMENDMENT B

	CLAIMS REMAINING AFTER AMENDMENT (Column 1)		HIGHEST NUMBER PREVIOUSLY PAID FOR (Column 2)	PRESENT EXTRA (Column 3)	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))	*	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
13/615,557	09/13/2012	2431	1250	077580-0177	20	2

CONFIRMATION NO. 1089

23630
McDermott Will & Emery
The McDermott Building
500 North Capitol Street, N.W.
Washington, DC 20001

UPDATED FILING RECEIPT

OC000000057854810

Date Mailed: 12/03/2012

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**

Inventor(s)

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

Applicant(s)

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

Assignment For Published Patent Application

VIRNETX, INC., Zephyr Cove, NV

Power of Attorney: The patent practitioners associated with Customer Number 22907

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 for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

If Required, Foreign Filing License Granted: 10/02/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/615,557**

Projected Publication Date: 03/14/2013

Non-Publication Request: No

Early Publication Request: No

Title

AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

Preliminary Class

713

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).

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 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
13/615,557	09/13/2012	Victor Larson	077580-0177

CONFIRMATION NO. 1089

PUBLICATION NOTICE

OC000000059856436

23630
McDermott Will & Emery
The McDermott Building
500 North Capitol Street, N.W.
Washington, DC 20001

Title:AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

Publication No.US-2013-0067224-A1
Publication Date:03/14/2013

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**077580-0177 (VRNK-0001CP3CON8)**

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
	A163	4,677,434	06/30/1987	Fascenda	
	A164	5,007,051	04/09/1991	Dolkas et al.	
	A165	5,345,439	09/06/1994	Marston	
	A166	5,838,796	11/17/1998	Mittenthal	
	A167	5,884,038	03/16/1999	Kapoor	
	A168	6,182,227	01/30/2001	Blair et al.	
	A169	6,266,699	07/24/2001	Sevcik	

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
	B22	US2002/0002675	01/03/2002	Bush	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3-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
	C25	JP 09-270803	10/14/1997	Furukawa Electric Co. Ltd.			
	C26	JP 10-111848	04/28/1998	AT&T Corp.			
	C27	JP 10-215244	08/11/1998	Sony Corp.			
	C28	JP 04-117826	04/17/1992	Matsushita Electric Ind. Co. Ltd.			

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.	
	D1254	Eastlake, "Domain Name System Security Extensions," Network Working Group, RFC: 2535 pages 2-11 (March 1999)	
	D1255	Press Release; VirnetX and Aastra Sign a Patent License Agreement, 4 pages, May 2012, Printed from Website: http://virnetx.com/virnetx-and-aastra-sign-a-patent-license-agreement/	
	D1256	Press Release; VirnetX and Mitel Networks Corporation Sign a Patent License Agreement, 5 pages, July 2012, Printed from Website: http://virnetx.com/virnetx-and-mitel-networks-corporation-sign-a-patent-license-agreement/	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**077580-0177 (VRNK-0001CP3CON8)**

	D1257	Press Relese; Virnetx and NEC Corporation and NEC Corporation of America Sign a Patent License Agreement, 5 pages, August 2012, Printed from Website: http://virnetx.com/virnetx-and-nec-corporation-and-nec-corporation-of-america-sign-a-patent-license-agreement/	
	D1258	Supplemental Declaration of Angelos D. Keromytis, Ph.D from Control No.: 95001789 pp. 1-18, dated December 20, 2012	
	D1259	Supplemental Declaration of Angelos D. Keromytis, Ph.D from Control No.: 95001851 pp. 1-13, dated December 30, 2012	
	D1260	Supplemental Declaration of Angelos D. Keromytis, Ph.D from Control No.: 95001788 pp. 1-18, dated December 18, 2012	
	D1261	Supplemental Declaration of Angelos D. Keromytis, Ph.D from Control No.: 95001856 pp. 1-13, dated December 30, 2012	
	D1262	VirnetX vs Apple Transcript of Trial, Afternoon Session, 12:05 p.m., dated November 5, 2012	
	D1263	Certified Copy dated September 18, 2012 of U.S. Patent Number 6,502,135, 73 pages	
	D1264	Certified Copy dated December 30, 2009 of Assignment for Patent Application Number 95/047,83 12 pages	
	D1265	Certified Copy dated March 11, 2008 of Patent Application Number 09/504,783, 1500 pages	
	D1266	Certified Copy dated March 30, 2011 of U.S. Patent Number 7,418,504, 74 pages	
	D1267	Certified Copy dated October 17, 2012 of Assignment for Patent Application Number: 10/714,849, 10 pages	
	D1268	Certified Copy dated April 4, 2011 of Patent Application Number 10/714,849, 1170 pages	
	D1269	Certified Copy dated March 30, 2011 of U.S. Patent Number 7,490,151, 63 pages	
	D1270	Certified Copy dated October 17, 2012 of Assignment for Patent Application Number 10/259,494, 19 pages	
	D1271	Certified Copy dated April 4, 2011 of Application Number 10/259,454, 1359 pages	
	D1272	Certified Copy dated April 12, 2011 of U.S. Patent Number 7,921,211, 78 pages	
	D1273	Certified Copy dated October 17, 2012 of Assignment for Application Number 11/840,560, 12 pages	
	D1274	Certified Copy dated April 20, 2011 of Application Number 11/840,560, 3 pages	
	D1275	iPhone User Guide for iPhone OS 3.1 Software, 217 pages, 2009	
	D1276	iPhone User Guide for iOS 4.2 and 4.3 Software, 274 pages, 2011	
	D1277	iPhone User Guide for iPhone and iPhone 3G, 154 pages, 2008	
	D1278	iPhone User Guide for iOS 5.0 Software, 163 pages, 2011	
	D1279	iPad User Guide for iOS 5.0 Software, 141 pages, 2011	
	D1280	iPad User Guide for iOS 4.2 Software, 181 pages, 2010	
	D1281	iPad User Guide for iOS 4.3 Software, 198 pages, 2011	
	D1282	iPad User Guide, 154 pages, 2010	
	D1283	iPod Touch User Guide for iOS 5.0 Software, 143 pages, 2011	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**077580-0177 (VRNK-0001CP3CON8)**

	D1284	iPod Touch User Guide, 122 pages, 2008	
	D1285	iPod Touch User Guide for iPhone OS 3.0 Software, 153 pages, 2009	
	D1286	iPod Touch User Guide for iPhone OS 3.1 Software, 169 pages, 2009	
	D1287	iPod Touch User Guide for iOS 4.3 Software, 230 pages, 2011	
	D1288	iPod Touch Features Guide, 98 pages, 2008	
	D1289	VPN Server Configuration for iOS; Networking & Internet Enterprise Deployment, 12 pages, 2011	
	D1290	iPhone Configuration Utility User Guide, 26 pages, 2010	
	D1291	iPhone Configuration Utility; Networking & Internet: Enterprise Deployment, 26 pages, 2011	
	D1292	iPhone Configuration Utility; Networking>Internet & Web, 24 pages, 2010	
	D1293	iOS Configuration Profile Reference; Networking & Internet: Enterprise Deployment, 24 pages, 2011	
	D1294	iPhone OS Enterprise Deployment Guide; Second Edition, for Version 3.1 or Later, 91 pages, 2009	
	D1295	iPhone OS; Enterprise Deployment Guide; Second Edition, for Version 3.2 or Later, 90 pages, 2010	
	D1296	CFHost Reference; Developer, 20 pages, 2008	
	D1297	CFNetwork Programming Guide; Developer, 60 pages, 2011	
	D1298	CFStream Socket Additions; Developer, 22 pages, 2010	
	D1299	Mac OS X Devloper Library; CFHostSample.c, 1 page	
	D1300	Mac OS X Developer Library; CFHostSample, 1 page, 2004	
	D1301	Mac OS X Developer Library; Document Revision History, 1 page, 2004	
	D1302	CFStream Socket Additions; Developer, 22 pages, 2010	
	D1303	Apple Push Notification Service; Distribution Service, Version 1.0, 6 pages, 2009	
	D1304	iOS Human Interface Guidelines; Developer, 184 pages, 2012	
	D1305	Networking & Internet Starting Point, 3 pages, 2011	
	D1306	Server Admin. 10.5 Help; Viewing a VPN Overview, 1 page	
	D1307	iOS: Supported Protocols for VPN, 2 pages, 2010	
	D1308	IPhone in Business Virtual Private Networks (VPN), 3 pages, 2010	
	D1309	iPhone and iPad in Business Deployment Scenarios, 26 pages, 2011	
	D1310	Deploying iPhone and iPad Virtual Private Networks, 3 pages, 2011	
	D1311	Deploying iPhone and iPad; Security Overview, 6 pages, 2011	
	D1312	Pad in Business; "Ready for Work," 2012, 5 pages	
	D1313	iOS: Using FaceTime, 2 pages, 2011, Printed from website http://support.apple.com/kb/HT4317	
	D1314	MobileMe: "Secure Chat" is Unavailable in OS X Lion, 2 pages, 2012, Printed from Website: http://support.apple.com/kb/TS3902	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**077580-0177 (VRNK-0001CP3CON8)**

	D1315	iPhone 4 and iPod Touch (4th Generation): Using FaceTime, 2 pages, 2010, Printed from Website: http://support.apple.com/kb/HT4319	
	D1316	IPhone; "Picking Up Where Amazing Left Off," 11 pages, 2012, Printed from Website: http://www.apple.com/iPhone/features/facetime	
	D1317	FaceTime for Mac; "Say Hello to FaceTime for Mac," 4 pages, 2012, Printed from Website: http://www.apple.com/mac/facetime	
	D1318	iPad; "Your New Favorite Way to do Just About Everything," 8 pages, 2012, Printed from Website" http://www.apple.com/ipad/built-in-apps/	
	D1319	iPod Touch; FaceTime, "Oh, I see what you're saying," 2 pages	
	D1320	Apple Press Info; Apple Presents iPhone 4, Printed from Website: http://www.apple.com/pr/library/apple-presents-iphone	
	D1321	iPod Touch; FaceTime, "Oh I See What You're Saying,", 3 pages, 2012, Printed from Website: http://www.apple.com/iPodtouch/built-in-apps/facetime.htm	
	D1322	IOS 4, The World's Most Advanced Mobile Operating System, 5 pages, Printed from Website: http://www.apple.com/iphone/ios4	
	D1323	Apple Press Info; Apple Reinvents the Phone with iPhone, 3 pages, 2007, Printed from Website: http://www.apple.com/pr/library/2007/01/09Apple-reinvents-the-phone	
	D1324	Apple Press Info; Apple Announces the New iPhone 3Gs-The Fastest, Most Powerful iPhone Yet, 3 pages, 2009, Printed from the Website: http://www.apple.com/pr/library/2009/06/08Apple-Announces-the-new-iphone3GS	
	D1325	Apple Press Info; Apple Launches iPhone 4S, ios 5 & iCloud, iPhone 4S Features Dual-Core A5 Chip, All New Camera, full 1080p HD Video Recording & Introduces Siri, 2011, 2 pages, Printed from website: http://www.apple.com/pr/library/2011/10/04Apple-Launches-iPhone-4S-iOS-5-iCloud.html	
	D1326	Apple Press Info; Apple Introduces New iPod Touch, Features Retina Display, A4 Chip, FaceTime Video Calling, HD Video Recording & Game Center, 2 pages, 2010, Printed from Website http://www.apple.com/pr/library/2010/09/01Apple-Introduces-New-iPod-touch.html	
	D1327	Apple Press Info; Apple Launches iPad, Magical & Revolutionary Device at an Unbelievable Price, 2 pages, 2010, Printed from Website: http://www.apple.com/pr/library/2010/01/27Apple-Launches-iPad.html	
	D1328	Apple Press Info; Apple Launces New iPad, New iPad Features Retina Display, A5X Chip, 5 Megapixel iSight Camera & Ultrafast 4G LTE, 2012, 3 pages, Printed from the Website: http://www.apple.com/pr/library/2012/03/07Apple-Launches-New-iPad.html	
	D1329	FaceTime; "Phone Calls Like You've Never Seen Before," 3 pages	
	D1330	Apple Press Info; Apple Brings FaceTime to the Mac, 1 pages, Printed from Website https://www.apple.com/pr/library/2010/10/20Apple-Brings-FaceTime-to-the-Mac.html	
	D1331	iPad at Work; "Mobile Meetings Made Easy," 4 pages, 2011	
	D1332	IPad – Technical Specifications, 49 pages, Printed from Website: http://support.apple.com/kb/sp58C	
	D1333	Stirling Design, 8 pages, 2008	
	D1334	Quick Guide: SSL VPN Technical Primer, 11 pages, 2010	
	D1335	Silva, "Secure iPhone Access to Corporate Web Applications," Technical Brief, 10 pages	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**077580-0177 (VRNK-0001CP3CON8)**

	D1336	Defendant Apple Inc.'s Third Supplemental Responses to VirnetX Inc.'s First Request for Admission to Apple Inc. dated, April 13, 2012, 207 pages	
	D1337	Apple Support Communities, 4 pages, Printed from Website https://discussions.apple.com/thread/486096?start=0&tstart=0	
	D1338	VirnetX – Products; License and Service Offerings, 1 page	
	D1339	VirnetX Contact Information, 4 pages, 2011	
	D1340	VirnetX Launches Secure Domain Name Initiative; 4G/LTE Security, 1 page, 2010	
	D1341	VirnetX Gabriel Connection; Enabling Safe Network Neighborhoods, 2 pages, 2012	
	D1342	Baugher et al., "The Secure Real-Time Transport Protocol (SRTP)," Network Working Group, RFC:3711, 39 pages, 2004	
	D1343	Jennings et al., "Resource Location and Discovery (Reload) Draft-Bryan-P2PSIP-Reload-04," Internet-Draft, 12/12/08, pages 1-127	
	D1344	Barnes et al., "Verification Involving PSTN Reachability: Requirements and Architecture Overview," Internet Draft, 27 pages, 2012	
	D1345	April Inc. Form 10-K (Annual Report) filed 12/01/05 for the Period Ending 09/24/05, Edgar Online, 1400 pages, 2011	
	D1346	Phone, Facetime; "Be in Two Places at Once," 3 pages, Printed from the Website http://www.apple.com/ios/facetime/	
	D1347	Apple Press Info; Apple Presents iPhone 4, All-New Design with FaceTime Video Calling, Retina, Display, 5 Megapixel Camera & HD Video Recording, 3 pages, 2010	
	D1348	NYSE AMEX:VHC; Cowen and Co. 39th Annual Technology Media & Telecom Conference, 36 pages, June 2, 2011	
	D1349	Pindyck et al., "Market Power: Monopoly and Monopsony," Microeconomics, Sixth Edition, pages 370-371	
	D1350	Press Release; IpCapital Group Completes VirnetX IP Licensing Evaluation, 3 pages	
	D1351	Microsoft Real-Time Communications: Protocols and Technologies, Microsoft TechNet, 22 pages, 2010	
	D1352	Filing Receipt dated September 23, 2011 for Application Number: 13/223,259	
	D1353	Email Communications Regarding Apple Product Innovations, 6 pages, 2010	
	D1354	Mathy et al., "Traversal Using Relays Around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)," Internet Engineering Task Force (IETF), RFC: 5766, 67 pages, 2010	
	D1355	Egevang et al., "The IP Network Address Translator (NAT)," Network Working Group, RFC: 1631, 10 pages, 1994	
	D1356	Srisuresh et al., "IP Network Address Translator (NAT) Terminology and Considerations," Network Working Group, RFC:2663, 30 pages, 1999	
	D1357	Sisalem, et al., "Introduction to Cryptographic Mechanisms," SIP Security, 356 pages, 2009	
	D1358	Curriculum Vitae, Mark T Jones, 9 pages	
	D1359	Curriculum Vitae, Roy Weinstein, 5 pages	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**077580-0177 (VRNK-0001CP3CON8)**

	D1360	How To Configure IPSec Tunneling in Windows 2000, 8 pages	
	D1361	Press Relese; Virnetx and NEC Corporation and NEC Corporation of America Sign a Patent License Agreement, 5 pages, August 2012, Printed from Website: http://virnetx.com/vimetx-and-nec-corporation-and-nec-corporation-of-america-sign-a-patent-license-agreement/	
	D1362	iPhone, FaceTime; "Be in Two Places at Once," 3 pages, Printed from Website: http://www.apple.com/ios/facetime/	
	D1363	iPhone, "It Does Everything Better,"6 pages, Printed from Website: http://www.apple.com/iPhone/built-in-apps	
	D1364	My Apple ID, "What's an Apple ID," 1 pages, Printed from Website: https://appleid.apple.com/cgi-bin/webobjects/myappleid.woa	
	D1365	Rosenberg et al., "Session Initiation Protocol (SIP): Locating SIP Servers," Network Working Group, RFC: 3263, 17 pages, 2002	
	D1366	Certified Copy dated September 21, 2012 of Reexamination Certificate Number 6,502,135 issued June 6, 2011, 11 pages	
	D1367	Certified Copy dated September 20, 2012 of Patent Application Number 95/001,269	
	D1368	Chatterjee et al., "Bargaining Under Incomplete Information," Operations Research, 31:835-851, 1983	
	D1369	Nash, "The Bargaining Problem," Econometrica, 18:155-162, 1950	
	D1370	Nash, "Two-Person Cooperative Games," Econometrica, 21:128-140, 1953	
	D1371	Choi et al., "An Analytical Solution to Reasonable Royalty Rate Calculations," IDEA: The Journal of Law and Technology, 13 pages, 2001	
	D1372	The Prize in Economics 1994 - Press Release dated October 11, 1994, 4 pages, Printed from Website: http://www.nobelprize.org/nobel_prizes/economics/laureates/1994/press.html	
	D1373	Putnam et al., "Bargaining and the Construction of Economically Consistent Hypothetical License Negotiations," The Licensing Journal, pages 8-15, 2004	
	D1374	Scherling et al., "Rational Reasonable Royalty Damages: A Return to the Roots," Landslide, Volume 4, 4 pages, 2011	
	D1375	Jarosz et al., "Application of Game Theory to Intellectual Property Royalty Negotiations," Chapter 17, pages 241-265	
	D1376	Goldscheider, Licensing Best Practices; Strategic, Territorial, and Technology Issues, 2 pages, 2006	
	D1377	iPhone Configuration Utility, 19 pages, 2012	
	D1378	VPN Server Configuration for iOS Devices, 6 pages, 2012	
	D1379	Samuelson et al., Economics, Fourteenth Edition, pages 258-259, 1992	
	D1380	Stigler et al., The Theory of Price, Forth Edition, pages 215-216, 1987	
	D1381	Truett et al., "Joint Profit Maximization, Negotiation, and the Determinacy of Price in Bilateral Monopoly," Journal of Economic Education, pages 260-270	
	D1382	Binmore et al., "Noncooperative Models of Bargaining," The Handbook of Game Theory, 1:(7)181-225,1992	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**077580-0177 (VRNK-0001CP3CON8)**

	D1383	Spindler et al., "Endogenous Bargaining Power in Bilateral Monopoly and Bilateral Exchange," Canadian Journal of Economics-Revue Canadienne D Economie, pages 464-474, 1974	
	D1384	Myerson, "Game Theory; Analysis or Conflict," Harvard University Press, pages 375-392	
	D1385	Binmore, "The Nash Bargaining Solution in Economic Modelling," The Rand Journal of Economics, 17:176-188, 1996	
	D1386	Rubinstein et al., "On the Interpretation of the Nash Bargaining Solution and its Extension to Non-Expected Utility Preferences," Econometrica, 60:1171-1186, 1992	
	D1387	Greenleaf et al., "Guarantees in Auctions: The Auction House as Negotiator and Managerial Decision Maker," Management Science, 39:1130-1145, 1993	
	D1388	Chan, "Trade Negotiations in a Nash Bargaining Model," Journal of International Economics, 25:253-363, 1987	
	D1389	Lemley et al., "Patent Holdup and Royalty Stacking," Texas Law Review, 85:1991-2049	
	D1390	Cauley, "Winning the Patent Damages Case; A Litigator's Guide to Economic Models and Other Damage Strategies," Oxford Press, pages 29-30, 2044	
	D1391	Degnan et al., "A Survey of Licensed Royalties," Les Nouvelles, pages 91, 93, 94, 1997	
	D1392	Kahn, "The Review of Economics and Statistics," pages 157-164, 1993	
	D1393	Microsoft Company Information; Including Stocks and Financial Information, 83 pages	
	D1394	Apple Press Info: Apple Updates MacBook Pro with Next Generation Processors, Graphics & Thunderbolt I/O Technology, 3 pages, Printed from Website: http://www.apple.com/pr/library/2011/02/24Apple-Updates-MacBook-Pro-with-Next-Generation-Processors-Graphics-Thunderbolt-I-O-Technology.html	
	D1395	Apple Press Info: Apple to Ship Mac OS X Snow Leopard on August 28, 2 pages, Printed from the Website: http://www.apple.com/pr/library/2009/08/24/apple-to-ship-mac-os-x	
	D1396	iPad, Facetime; "Once Again, iPad gets the World Talking," 3 pages, Printed from the Website: http://www.apple.com/ipad/built-in-apps/facetime/html	
	D1397	Apple iOS: Setting up VPN, 2 pages, Printed from Website: http/support.apple.com/kb/HT1424	
	D1398	Apple iPhone User Guide for iOS 5.1 Software, 179 pages, 2012	
	D1399	Apple, Communicating with HTTP Servers, CFNetworking Programming Guide, 6 pages, 2011, Printed from the Website: https://developer.apple.com/library/ios/documentation/networking/conceptual/CFNetwork/CFHT	
	D1400	VirnetX, Gabriel Connection Technology ™ White Paper, 7 pages, 2012	
	D1401	VirnetX, Technology, 4 pages, 2012	
	D1402	Certified Copy dated January 15, 2008 of U.S. Patent Number 6,502,135, 64 pages	
	D1403	Inter Partes Reexamination Certificate dated June 7, 2011 for Patent Number 6,502,135	
	D1404	Proceedings of The Symposium on Network and Distributed System Security, 7 pages, February 22-23, 1996	
	D1405	In-Q-Tel; Corporate Overview, 2 pages, 2004	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**077580-0177 (VRNK-0001CP3CON8)**

	D1406	Davies, Supervisor of Translation: Tadahiro Uezono, Security for Computer Networks, Japan, Nikkei-McGraw-Hill Inc., First Edition, First Copy, p 126-129 (December 5, 1985) – (English Version and Japanese Version Submitted)	
	D1407	Comer, "Translated by Jun Murai and Hiroyuki Kusumoto, "Internetworking with TCP/IP Vol. 1: Principles, Protocols, and Architecture, Third Edition," Japan Kyoritsu Shuppan Co., Ltd., First Edition, First Copy, p 161-193 (August 10, 1997) (English Version and Japanese Version Submitted)	
	D1408	Lynch et al., Supervisor of Translation: Jun Murai, "Internet System Handbook," Japan Impress Co. Ltd. First Edition p 152-157 and p 345-351 (August 11, 1996) (English Version and Japanese Version Submitted)	
	D1409	Office Action dated December 27, 2012 from Corresponding Canadian Patent Application Number 2723504	
	D1410	Office Action dated December 5, 2012 from Corresponding Japanese Patent Application Number 2011-081417	
	D1411	Office Action dated December 13, 2012 from Corresponding Japanese Patent Application Number 2011-085052	
	D1412	Office Action dated December 13, 2012 from Corresponding Japanese Patent Application Number 2011-083415	

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 **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**077580-0177 (VRNK-0001CP3CON8)**

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.

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[X] 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.

[ ] 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 any required fees 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 $930.00, 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/ Date: April 9, 2013

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 42160652-1.077580.0177

Electronic Acknowledgement Receipt

EFS ID:	15467015
Application Number:	13615557
International Application Number:	
Confirmation Number:	1089
Title of Invention:	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:	077580-0177
Receipt Date:	09-APR-2013
Filing Date:	13-SEP-2012
Time Stamp:	11:23:01
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)	177IDS.pdf	725608 6bbec1410890a62d0c6afe8cc7b031a54d043656	no	9

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

Total Files Size (in bytes):	725608

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 NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/615,557	09/13/2012	Victor Larson	077580-0177	1089

23630 7590 08/01/2013

McDermott Will & Emery
The McDermott Building
500 North Capitol Street, N.W.
Washington, DC 20001

EXAMINER	
LIM, KRISNA	
ART UNIT	**PAPER NUMBER**
2453	

NOTIFICATION DATE	DELIVERY MODE
08/01/2013	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. 13/615,557	Applicant(s) LARSON ET AL.	
	Examiner KRISNA LIM	Art Unit 2453	AIA (First Inventor to File) Status No

-- 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 *13 September 2012*.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

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) *1-20* 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) *1-20* is/are rejected.
8)☐ Claim(s) _____ is/are objected to.
9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

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).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some * c)☐ None of the:
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) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
4) ☐ Other: _____.

1. Claims 1-20 are presented for examination.

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 1-20 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-18 of U.S. Patent No. 7,933,990.

Although the conflicting claims are not identical, they are not patentably distinct from each other because they all directed to a method of transparently creating an encrypted communication channel (i.e. **automatically initiating** an encrypted communication channel) between a client device and a target device based on a determination that a request access to a device that accepts an encrypted communication channel. The difference is the current application claimed language of **"supports secure communications audio/video"**. It would have been obvious to one of ordinary skill in the art to recognize that such additional claimed language" **supports communications audio/video"** would have been a matter of use and such feature is well known and it would not be a patentably distinguishable feature.

4. Claims 1-20 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-3, 5-9 and 11-15 of U.S. Patent No. 7,490,151.

Although the conflicting claims are not identical, they are not patentably distinct from each other because they are directed to a method **of transparently creating** an encrypted communication channel (i.e. **automatically initiating** an encrypted communication channel) between a client device and a target device based on a determination that a request access to a device that accepts an encrypted communication channel. The difference is the current application claimed language of **"supports secure communications audio/video"**. It would have been obvious to one of ordinary skill in the art to recognize that such additional claimed language" **supports communications audio/video"** would have been a matter of use and such feature is well known and it would not be a patentably distinguishable feature.

5. Claims 1-19 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-9 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 method of transparently creating an encrypted communication channel (i.e. **transparently creating a virtual private network**) between a client device and a target device based on a determination that a request access to a device that accepts an encrypted communication channel. The difference is the current application claimed language of **"supports secure communications audio/video"**. It would have been obvious to one of ordinary skill in the art to recognize that such additional claimed language" **supports communications audio/video"** would have been a matter of use and such feature is well known and it would not be a patentably distinguishable feature.

6. 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.

7. 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.

8. Claims 1-20 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Wesinger [U.S. Patent No. 5,898,830].

9. Wesinger disclosed the invention substantially as claimed. Taking claims 1-4, 10-12 and 19-20 as exemplary claims, the reference disclose a client device comprising: a) memory configured and arranged to facilitate a connection (i.e., see Internet 120 of Fig. 1) of the client device (i.e. a client C) with a target device (i.e. a host D) over a <u>secure communication link created</u> (i.e., at 12:23-27 Wesinger disclosed "... **combining encryption capabilities .... allows for the creation of virtual private networks-networks in which two remote machine communicate securely** ...") based on (i) an <u>address request generated by the client device</u> (i.e., see 9:1-25), and (ii) a

determination as a result of the address request that the target device is a device with which a secure communication link can be established (i.e. at 12:4-47, Wesinger disclosed channel processing may be used to perform virus protection.... Encryption and decryption are particularly important to .... **Internet and network communication … encryption could be performed**”) when the requested address is identified in an address lookup (i.e. at 8:25-9:25, Wesinger disclosed “... DNS is a ... system that translates host name address to IP address and IP address to host name ... stored in DNS tables ... When client C tries to initiates a connection to host D .... The DNS server for D returns the network address D ... from which it receives the look up request ...” Moreover see Wesinger's teaching at 9:53-60, 16:57-17:5, 12:23-27),

wherein the establishment of the secure communication link (i.e., at 12:23-27 Wesinger disclosed "... **combining encryption capabilities .... allows for the creation of virtual private networks-networks in which two remote machine communicate securely** ...") is based on a determination being made by a proxy module (i.e., a proxy server) that the target device is a device with which a secure communication link can be established when the address request corresponds to a target device identified in a DNS lookup table (i.e. Wesinger disclosed at col. 8 (line 25) to col. 9 (line 25) " ... DNS is a ... system that translates host name address to IP address and IP address to host name ... stored in DNS tables ... When client C tries to initiates a connection to host D .... The DNS server for D returns the network address D ... from which it receives the look up request ...” Moreover, see col. 8 (lines 33-48), col. 8 (line 65) to col. 9 (line 2), col. 9 (lines 19-25), col. 16 (line 57) to col. 17 (line 5) and col. 12 (lines 23-27)),

wherein the address lookup is a network address lookup (i.e. Wesinger disclosed at col. 8 (line 25) to col. 9 (line 25) " ... DNS is a ... system that translates host name address to IP address and IP address to host name ... stored in DNS tables ... When client C tries to initiates a connection to host D .... The DNS server for D returns the network address D ... from which it receives the look up request ...”;

wherein the secure communication link is a virtual private network link (i.e., Wesinger at col. 12 (lines 23-27) disclosed "... **combining encryption capabilities ....**

allows for the creation of virtual private networks-networks in which two remote machine communicate securely ..."); and

wherein the address request includes a secure domain name (i.e., see DNS of figure 1 and columns 8-9).

10. Wesinger did not explicitly mention a specific application program configured and arranged so as to allow participation in audio/video communications with the target device over the secure communication link, it would however have been obvious to one of ordinary skill in the art at the time the invention was made to recognize that having such audio/video application to communicate over the secure communication link would have been a matter of choice, and it would not be a patentably distinguishable feature.

11. As to claims 5-9 and 13-18, those features (i.e., a computer, a server, a phone, a broadband connection, TCP/IP protocols support, using modulation based on FDM, TDM, or CDMA, etc.) are well known the art at the time the invention was made and they are not patentably distinguishable features.

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.

Kl
July 25, 2013

/Krisna Lim/
Primary Examiner Art Unit 2453

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13615557	LARSON ET AL.
	Examiner	**Art Unit**
	KRISNA LIM	2453

CPC- SEARCHED

Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED

Symbol	Date	Examiner

US CLASSIFICATION SEARCHED

Class	Subclass	Date	Examiner
709	222-227	07/25/2013	kl

SEARCH NOTES

Search Notes	Date	Examiner
Inventors	07/25/2013	kl

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**077580-0177 (VRNK-0001CP3CON8)**

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
	A163	4,677,434	06/30/1987	Fascenda	
	A164	5,007,051	04/09/1991	Dolkas et al.	
	A165	5,345,439	09/06/1994	Marston	
	A166	5,838,796	11/17/1998	Mittenthal	
	A167	5,884,038	03/16/1999	Kapoor	
	A168	6,182,227	01/30/2001	Blair et al.	
	A169	6,266,699	07/24/2001	Sevcik	

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
	B22	US2002/0002675	01/03/2002	Bush	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code-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
	C25	JP 09-270803	10/14/1997	Furukawa Electric Co. Ltd.			
	C26	JP 10-111848	04/28/1998	AT&T Corp.			
	C27	JP 10-215244	08/11/1998	Sony Corp.			
	C28	JP 04-117826	04/17/1992	Matsushita Electric Ind. Co. Ltd.			

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.	
	D1254	Eastlake, "Domain Name System Security Extensions," Network Working Group, RFC: 2535 pages 2-11 (March 1999)	
	D1255	Press Release; VirnetX and Aastra Sign a Patent License Agreement, 4 pages, May 2012, Printed from Website: http://virnetx.com/virnetx-and-aastra-sign-a-patent-license-agreement/	
	D1256	Press Release; VirnetX and Mitel Networks Corporation Sign a Patent License Agreement, 5 pages, July 2012, Printed from Website: http://virnetx.com/virnetx-and-mitel-networks-corporation-sign-a-patent-license-agreement/	

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	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**077580-0177 (VRNK-0001CP3CON8)**

	D1257	Press Relese; Virnetx and NEC Corporation and NEC Corporation of America Sign a Patent License Agreement, 5 pages, August 2012, Printed from Website: http://virnetx.com/virnetx-and-nec-corporation-and-nec-corporation-of-america-sign-a-patent-license-agreement/	
	D1258	Supplemental Declaration of Angelos D. Keromytis, Ph.D from Control No.: 95001789 pp. 1-18, dated December 20, 2012	
	D1259	Supplemental Declaration of Angelos D. Keromytis, Ph.D from Control No.: 95001851 pp. 1-13, dated December 30, 2012	
	D1260	Supplemental Declaration of Angelos D. Keromytis, Ph.D from Control No.: 95001788 pp. 1-18, dated December 18, 2012	
	D1261	Supplemental Declaration of Angelos D. Keromytis, Ph.D from Control No.: 95001856 pp. 1-13, dated December 30, 2012	
	D1262	VirnetX vs Apple Transcript of Trial, Afternoon Session, 12:05 p.m., dated November 5, 2012	
	D1263	Certified Copy dated September 18, 2012 of U.S. Patent Number 6,502,135, 73 pages	
	D1264	Certified Copy dated December 30, 2009 of Assignment for Patent Application Number 95/047,83 12 pages	
	D1265	Certified Copy dated March 11, 2008 of Patent Application Number 09/504,783, 1500 pages	
	D1266	Certified Copy dated March 30, 2011 of U.S. Patent Number 7,418,504, 74 pages	
	D1267	Certified Copy dated October 17, 2012 of Assignment for Patent Application Number: 10/714,849, 10 pages	
	D1268	Certified Copy dated April 4, 2011 of Patent Application Number 10/714,849, 1170 pages	
	D1269	Certified Copy dated March 30, 2011 of U.S. Patent Number 7,490,151, 63 pages	
	D1270	Certified Copy dated October 17, 2012 of Assignment for Patent Application Number 10/259,494, 19 pages	
	D1271	Certified Copy dated April 4, 2011 of Application Number 10/259,454, 1359 pages	
	D1272	Certified Copy dated April 12, 2011 of U.S. Patent Number 7,921,211, 78 pages	
	D1273	Certified Copy dated October 17, 2012 of Assignment for Application Number 11/840,560, 12 pages	
	D1274	Certified Copy dated April 20, 2011 of Application Number 11/840,560, 3 pages	
	D1275	iPhone User Guide for iPhone OS 3.1 Software, 217 pages, 2009	
	D1276	iPhone User Guide for iOS 4.2 and 4.3 Software, 274 pages, 2011	
	D1277	iPhone User Guide for iPhone and iPhone 3G, 154 pages, 2008	
	D1278	iPhone User Guide for iOS 5.0 Software, 163 pages, 2011	
	D1279	iPad User Guide for iOS 5.0 Software, 141 pages, 2011	
	D1280	iPad User Guide for iOS 4.2 Software, 181 pages, 2010	
	D1281	iPad User Guide for iOS 4.3 Software, 198 pages, 2011	
	D1282	iPad User Guide, 154 pages, 2010	
	D1283	iPod Touch User Guide for iOS 5.0 Software, 143 pages, 2011	

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	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**077580-0177 (VRNK-0001CP3CON8)**

	D1284	iPod Touch User Guide, 122 pages, 2008	
	D1285	iPod Touch User Guide for iPhone OS 3.0 Software, 153 pages, 2009	
	D1286	iPod Touch User Guide for iPhone OS 3.1 Software, 169 pages, 2009	
	D1287	iPod Touch User Guide for iOS 4.3 Software, 230 pages, 2011	
	D1288	iPod Touch Features Guide, 98 pages, 2008	
	D1289	VPN Server Configuration for iOS; Networking & Internet Enterprise Deployment, 12 pages, 2011	
	D1290	iPhone Configuration Utility User Guide, 26 pages, 2010	
	D1291	iPhone Configuration Utility; Networking & Internet: Enterprise Deployment, 26 pages, 2011	
	D1292	iPhone Configuration Utility; Networking>Internet & Web, 24 pages, 2010	
	D1293	iOS Configuration Profile Reference; Networking & Internet: Enterprise Deployment, 24 pages, 2011	
	D1294	iPhone OS Enterprise Deployment Guide; Second Edition, for Version 3.1 or Later, 91 pages, 2009	
	D1295	iPhone OS; Enterprise Deployment Guide; Second Edition, for Version 3.2 or Later, 90 pages, 2010	
	D1296	CFHost Reference; Developer, 20 pages, 2008	
	D1297	CFNetwork Programming Guide; Developer, 60 pages, 2011	
	D1298	CFStream Socket Additions; Developer, 22 pages, 2010	
	D1299	Mac OS X Devloper Library; CFHostSample.c, 1 page	
	D1300	Mac OS X Developer Library; CFHostSample, 1 page, 2004	
	D1301	Mac OS X Developer Library; Document Revision History, 1 page, 2004	
	D1302	CFStream Socket Additions; Developer, 22 pages, 2010	
	D1303	Apple Push Notification Service; Distribution Service, Version 1.0, 6 pages, 2009	
	D1304	iOS Human Interface Guidelines; Developer, 184 pages, 2012	
	D1305	Networking & Internet Starting Point, 3 pages, 2011	
	D1306	Server Admin. 10.5 Help; Viewing a VPN Overview, 1 page	
	D1307	iOS: Supported Protocols for VPN, 2 pages, 2010	
	D1308	IPhone in Business Virtual Private Networks (VPN), 3 pages, 2010	
	D1309	iPhone and iPad in Business Deployment Scenarios, 26 pages, 2011	
	D1310	Deploying iPhone and iPad Virtual Private Networks, 3 pages, 2011	
	D1311	Deploying iPhone and iPad; Security Overview, 6 pages, 2011	
	D1312	Pad in Business; "Ready for Work," 2012, 5 pages	
	D1313	iOS: Using FaceTime, 2 pages, 2011, Printed from website http://support.apple.com/kb/HT4317	
	D1314	MobileMe: "Secure Chat" is Unavailable in OS X Lion, 2 pages, 2012, Printed from Website: http://support.apple.com/kb/TS3902	

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	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**077580-0177 (VRNK-0001CP3CON8)**

	D1315	iPhone 4 and iPod Touch (4th Generation): Using FaceTime, 2 pages, 2010, Printed from Website: http://support.apple.com/kb/HT4319	
	D1316	IPhone; "Picking Up Where Amazing Left Off," 11 pages, 2012, Printed from Website: http://www.apple.com/iPhone/features/facetime	
	D1317	FaceTime for Mac; "Say Hello to FaceTime for Mac," 4 pages, 2012, Printed from Website: http://www.apple.com/mac/facetime	
	D1318	iPad; "Your New Favorite Way to do Just About Everything," 8 pages, 2012, Printed from Website" http://www.apple.com/ipad/built-in-apps/	
	D1319	iPod Touch; FaceTime, "Oh, I see what you're saying," 2 pages	
	D1320	Apple Press Info; Apple Presents iPhone 4, Printed from Website: http://www.apple.com/pr/library/apple-presents-iphone	
	D1321	iPod Touch; FaceTime, "Oh I See What You're Saying,", 3 pages, 2012, Printed from Website: http://www.apple.com/iPodtouch/built-in-apps/facetime.htm	
	D1322	IOS 4, The World's Most Advanced Mobile Operating System, 5 pages, Printed from Website: http://www.apple.com/iphone/ios4	
	D1323	Apple Press Info; Apple Reinvents the Phone with iPhone, 3 pages, 2007, Printed from Website: http://www.apple.com/pr/library/2007/01/09Apple-reinvents-the-phone	
	D1324	Apple Press Info; Apple Announces the New iPhone 3Gs-The Fastest, Most Powerful iPhone Yet, 3 pages, 2009, Printed from the Website: http://www.apple.com/pr/library/2009/06/08Apple-Announces-the-new-iphone3GS	
	D1325	Apple Press Info; Apple Launches iPhone 4S, ios 5 & iCloud, iPhone 4S Features Dual-Core A5 Chip, All New Camera, full 1080p HD Video Recording & Introduces Siri, 2011, 2 pages, Printed from website: http://www.apple.com/pr/library/2011/10/04Apple-Launches-iPhone-4S-iOS-5-iCloud.html	
	D1326	Apple Press Info; Apple Introduces New iPod Touch, Features Retina Display, A4 Chip, FaceTime Video Calling, HD Video Recording & Game Center, 2 pages, 2010, Printed from Website http://www.apple.com/pr/library/2010/09/01Apple-Introduces-New-iPod-touch.html	
	D1327	Apple Press Info; Apple Launches iPad, Magical & Revolutionary Device at an Unbelievable Price, 2 pages, 2010, Printed from Website: http://www.apple.com/pr/library/2010/01/27Apple-Launches-iPad.html	
	D1328	Apple Press Info; Apple Launces New iPad, New iPad Features Retina Display, A5X Chip, 5 Megapixel iSight Camera & Ultrafast 4G LTE, 2012, 3 pages, Printed from the Website: http://www.apple.com/pr/library/2012/03/07Apple-Launches-New-iPad.html	
	D1329	FaceTime; "Phone Calls Like You've Never Seen Before," 3 pages	
	D1330	Apple Press Info; Apple Brings FaceTime to the Mac, 1 pages, Printed from Website https://www.apple.com/pr/library/2010/10/20Apple-Brings-FaceTime-to-the-Mac.html	
	D1331	iPad at Work; "Mobile Meetings Made Easy," 4 pages, 2011	
	D1332	IPad – Technical Specifications, 49 pages, Printed from Website: http://support.apple.com/kb/sp58C	
	D1333	Stirling Design, 8 pages, 2008	
	D1334	Quick Guide: SSL VPN Technical Primer, 11 pages, 2010	
	D1335	Silva, "Secure iPhone Access to Corporate Web Applications," Technical Brief, 10 pages	

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	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**077580-0177 (VRNK-0001CP3CON8)**

	D1336	Defendant Apple Inc.'s Third Supplemental Responses to VirnetX Inc.'s First Request for Admission to Apple Inc. dated, April 13, 2012, 207 pages	
	D1337	Apple Support Communities, 4 pages, Printed from Website https://discussions.apple.com/thread/486096?start=0&tstart=0	
	D1338	VirnetX – Products; License and Service Offerings, 1 page	
	D1339	VirnetX Contact Information, 4 pages, 2011	
	D1340	VirnetX Launches Secure Domain Name Initiative; 4G/LTE Security, 1 page, 2010	
	D1341	VirnetX Gabriel Connection; Enabling Safe Network Neighborhoods, 2 pages, 2012	
	D1342	Baugher et al., "The Secure Real-Time Transport Protocol (SRTP)," Network Working Group, RFC:3711, 39 pages, 2004	
	D1343	Jennings et al., "Resource Location and Discovery (Reload) Draft-Bryan-P2PSIP-Reload-04," Internet-Draft, 12/12/08, pages 1-127	
	D1344	Barnes et al., "Verification Involving PSTN Reachability: Requirements and Architecture Overview," Internet Draft, 27 pages, 2012	
	D1345	April Inc. Form 10-K (Annual Report) filed 12/01/05 for the Period Ending 09/24/05, Edgar Online, 1400 pages, 2011	
	D1346	Phone, Facetime; "Be in Two Places at Once," 3 pages, Printed from the Website http://www.apple.com/ios/facetime/	
	D1347	Apple Press Info; Apple Presents iPhone 4, All-New Design with FaceTime Video Calling, Retina, Display, 5 Megapixel Camera & HD Video Recording, 3 pages, 2010	
	D1348	NYSE AMEX:VHC; Cowen and Co. 39th Annual Technology Media & Telecom Conference, 36 pages, June 2, 2011	
	D1349	Pindyck et al., "Market Power: Monopoly and Monopsony," Microeconomics, Sixth Edition, pages 370-371	
	D1350	Press Release; IpCapital Group Completes VirnetX IP Licensing Evaluation, 3 pages	
	D1351	Microsoft Real-Time Communications: Protocols and Technologies, Microsoft TechNet, 22 pages, 2010	
	D1352	Filing Receipt dated September 23, 2011 for Application Number: 13/223,259	
	D1353	Email Communications Regarding Apple Product Innovations, 6 pages, 2010	
	D1354	Mathy et al., "Traversal Using Relays Around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)," Internet Engineering Task Force (IETF), RFC: 5766, 67 pages, 2010	
	D1355	Egevang et al., "The IP Network Address Translator (NAT)," Network Working Group, RFC: 1631, 10 pages, 1994	
	D1356	Srisuresh et al., "IP Network Address Translator (NAT) Terminology and Considerations," Network Working Group, RFC:2663, 30 pages, 1999	
	D1357	Sisalem, et al., "Introduction to Cryptographic Mechanisms," SIP Security, 356 pages, 2009	
	D1358	Curriculum Vitae, Mark T Jones, 9 pages	
	D1359	Curriculum Vitae, Roy Weinstein, 5 pages	

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	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**077580-0177 (VRNK-0001CP3CON8)**

	D1360	How To Configure IPSec Tunneling in Windows 2000, 8 pages	
	D1361	Press Relese; Virnetx and NEC Corporation and NEC Corporation of America Sign a Patent License Agreement, 5 pages, August 2012, Printed from Website: http://virnetx.com/vimetx-and-nec-corporation-and-nec-corporation-of-america-sign-a-patent-license-agreement/	
	D1362	iPhone, FaceTime; "Be in Two Places at Once," 3 pages, Printed from Website: http://www.apple.com/ios/facetime/	
	D1363	iPhone, "It Does Everything Better,"6 pages, Printed from Website: http://www.apple.com/iPhone/built-in-apps	
	D1364	My Apple ID, "What's an Apple ID," 1 pages, Printed from Website: https://appleid.apple.com/cgi-bin/webobjects/myappleid.woa	
	D1365	Rosenberg et al., "Session Initiation Protocol (SIP): Locating SIP Servers," Network Working Group, RFC: 3263, 17 pages, 2002	
	D1366	Certified Copy dated September 21, 2012 of Reexamination Certificate Number 6,502,135 issued June 6, 2011, 11 pages	
	D1367	Certified Copy dated September 20, 2012 of Patent Application Number 95/001,269	
	D1368	Chatterjee et al., "Bargaining Under Incomplete Information," Operations Research, 31:835-851, 1983	
	D1369	Nash, "The Bargaining Problem," Econometrica, 18:155-162, 1950	
	D1370	Nash, "Two-Person Cooperative Games," Econometrica, 21:128-140, 1953	
	D1371	Choi et al., "An Analytical Solution to Reasonable Royalty Rate Calculations," IDEA: The Journal of Law and Technology, 13 pages, 2001	
	D1372	The Prize in Economics 1994 - Press Release dated October 11, 1994, 4 pages, Printed from Website: http://www.nobelprize.org/nobel_prizes/economics/laureates/1994/press.html	
	D1373	Putnam et al., "Bargaining and the Construction of Economically Consistent Hypothetical License Negotiations," The Licensing Journal, pages 8-15, 2004	
	D1374	Scherling et al., "Rational Reasonable Royalty Damages: A Return to the Roots," Landslide, Volume 4, 4 pages, 2011	
	D1375	Jarosz et al., "Application of Game Theory to Intellectual Property Royalty Negotiations," Chapter 17, pages 241-265	
	D1376	Goldscheider, Licensing Best Practices; Strategic, Territorial, and Technology Issues, 2 pages, 2006	
	D1377	iPhone Configuration Utility, 19 pages, 2012	
	D1378	VPN Server Configuration for iOS Devices, 6 pages, 2012	
	D1379	Samuelson et al., Economics, Fourteenth Edition, pages 258-259, 1992	
	D1380	Stigler et al., The Theory of Price, Forth Edition, pages 215-216, 1987	
	D1381	Truett et al., "Joint Profit Maximization, Negotiation, and the Determinacy of Price in Bilateral Monopoly," Journal of Economic Education, pages 260-270	
	D1382	Binmore et al., "Noncooperative Models of Bargaining," The Handbook of Game Theory, 1:(7)181-225,1992	

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	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**077580-0177 (VRNK-0001CP3CON8)**

	D1383	Spindler et al., "Endogenous Bargaining Power in Bilateral Monopoly and Bilateral Exchange," Canadian Journal of Economics-Revue Canadienne D Economie, pages 464-474, 1974	
	D1384	Myerson, "Game Theory; Analysis or Conflict," Harvard University Press, pages 375-392	
	D1385	Binmore, "The Nash Bargaining Solution in Economic Modelling," The Rand Journal of Economics, 17:176-188, 1996	
	D1386	Rubinstein et al., "On the Interpretation of the Nash Bargaining Solution and its Extension to Non-Expected Utility Preferences," Econometrica, 60:1171-1186, 1992	
	D1387	Greenleaf et al., "Guarantees in Auctions: The Auction House as Negotiator and Managerial Decision Maker," Management Science, 39:1130-1145, 1993	
	D1388	Chan, "Trade Negotiations in a Nash Bargaining Model," Journal of International Economics, 25:253-363, 1987	
	D1389	Lemley et al., "Patent Holdup and Royalty Stacking," Texas Law Review, 85:1991-2049	
	D1390	Cauley, "Winning the Patent Damages Case; A Litigator's Guide to Economic Models and Other Damage Strategies," Oxford Press, pages 29-30, 2044	
	D1391	Degnan et al., "A Survey of Licensed Royalties," Les Nouvelles, pages 91, 93, 94, 1997	
	D1392	Kahn, "The Review of Economics and Statistics," pages 157-164, 1993	
	D1393	Microsoft Company Information; Including Stocks and Financial Information, 83 pages	
	D1394	Apple Press Info: Apple Updates MacBook Pro with Next Generation Processors, Graphics & Thunderbolt I/O Technology, 3 pages, Printed from Website: http://www.apple.com/pr/library/2011/02/24Apple-Updates-MacBook-Pro-with-Next-Generation-Processors-Graphics-Thunderbolt-I-O-Technology.html	
	D1395	Apple Press Info: Apple to Ship Mac OS X Snow Leopard on August 28, 2 pages, Printed from the Website: http://www.apple.com/pr/library/2009/08/24/apple-to-ship-mac-os-x	
	D1396	iPad, Facetime; "Once Again, iPad gets the World Talking," 3 pages, Printed from the Website: http://www.apple.com/ipad/built-in-apps/facetime/html	
	D1397	Apple iOS: Setting up VPN, 2 pages, Printed from Website: http/support.apple.com/kb/HT1424	
	D1398	Apple iPhone User Guide for iOS 5.1 Software, 179 pages, 2012	
	D1399	Apple, Communicating with HTTP Servers, CFNetworking Programming Guide, 6 pages, 2011, Printed from the Website: https://developer.apple.com/library/ios/documentation/networking/conceptual/CFNetwork/CFHT	
	D1400	VirnetX, Gabriel Connection Technology ™ White Paper, 7 pages, 2012	
	D1401	VirnetX, Technology, 4 pages, 2012	
	D1402	Certified Copy dated January 15, 2008 of U.S. Patent Number 6,502,135, 64 pages	
	D1403	Inter Partes Reexamination Certificate dated June 7, 2011 for Patent Number 6,502,135	
	D1404	Proceedings of The Symposium on Network and Distributed System Security, 7 pages, February 22-23, 1996	
	D1405	In-Q-Tel; Corporate Overview, 2 pages, 2004	

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	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**077580-0177 (VRNK-0001CP3CON8)**

	D1406	Davies, Supervisor of Translation: Tadahiro Uezono, Security for Computer Networks, Japan, Nikkei-McGraw-Hill Inc., First Edition, First Copy, p 126-129 (December 5, 1985) – (English Version and Japanese Version Submitted)	
	D1407	Comer, "Translated by Jun Murai and Hiroyuki Kusumoto, "Internetworking with TCP/IP Vol. 1: Principles, Protocols, and Architecture, Third Edition," Japan Kyoritsu Shuppan Co., Ltd., First Edition, First Copy, p 161-193 (August 10, 1997) (English Version and Japanese Version Submitted)	
	D1408	Lynch et al., Supervisor of Translation: Jun Murai, "Internet System Handbook," Japan Impress Co. Ltd. First Edition p 152-157 and p 345-351 (August 11, 1996) (English Version and Japanese Version Submitted)	
	D1409	Office Action dated December 27, 2012 from Corresponding Canadian Patent Application Number 2723504	
	D1410	Office Action dated December 5, 2012 from Corresponding Japanese Patent Application Number 2011-081417	
	D1411	Office Action dated December 13, 2012 from Corresponding Japanese Patent Application Number 2011-085052	
	D1412	Office Action dated December 13, 2012 from Corresponding Japanese Patent Application Number 2011-083415	

EXAMINER /Krisna Lim/	DATE CONSIDERED 07/24/2013

*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 with no date, there are no date provided. /K.L./

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	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**077580-0177 (VRNK-0001CP3CON8)**

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.

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[X] 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.

[ ] 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 any required fees 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 $930.00, 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/

Date: April 9, 2013

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 42160652-1.077580.0177

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

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. 1089

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/615,557	09/13/2012 **RULE**	713	2453	077580-0177

APPLICANTS

Victor Larson, Fairfax, VA;
Robert Dunham Short III, Leesburg, VA;
Edmund 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 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** *************************

** **IF REQUIRED, FOREIGN FILING LICENSE GRANTED** **
10/02/2012

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	20	2

ADDRESS

McDermott Will & Emery
The McDermott Building
500 North Capitol Street, N.W.
Washington, DC 20001
UNITED STATES

TITLE

AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

FILING FEE RECEIVED		
1250	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

BIB (Rev. 05/07).

Index of Claims	Application/Control No. 13615557	Applicant(s)/Patent Under Reexamination LARSON ET AL.
	Examiner KRISNA LIM	Art Unit 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	07/25/2013								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	13/615,557
Filing Dates	September 13, 2012
First Named Inventor	Victor Larson
Art Unit	2431
Examiner Name	Not Yet Assigned
Docket Number	77580-177 (VRNK-0001CP3CON8)

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication/Patent Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1	09/399,753	09/22/1998	Graig Miller et al.	
	A2	60/151,563	08/31/1999	Bryan Whittles	
	A3	60/134,547	05/17/1999	Victory Sheymov	
	A4	2,895,502	07/21/1959	Roper et al.	
	A5	4,761,334	08/1988	Sagoi et al.	
	A6	4,885,778	12/5/1989	Weiss, Kenneth	
	A7	4,920,484	4/24/1990	Ranade	
	A8	4,933,846	06/12/1990	Humphrey et al.	
	A9	4,952,930	08/28/1990	Franaszek et al.	
	A10	4,988,990	01/29/1991	Warrior	
	A11	5,164,988	11/17/1992	Matyas	
	A12	5,204,961	04/20/1993	Barlow	
	A13	5,276,735	01/04/1994	Boebert et al	
	A14	5,303,302	04/12/1994	Burrows	
	A15	5,311,593	05/10/1994	Carmi	
	A16	5,329,521	07/12/1994	Walsh et al.	
	A17	5,341,426	08/23/1994	Barney et al.	
	A18	5,367,643	11/22/1994	Chang et al	
	A19	5,384,848	01/24/1995	Kikuchi	
	A20	5,511,122	04/23/1996	Atkinson	
	A21	5,548,646	08/20/1996	Aziz et al.	
	A22	5,559,883	09/24/1996	Williams	
	A23	5,561,669	10/01/1996	Lenney et al	
	A24	5,588,060	12/24/1996	Aziz	
	A25	5,590,285	12/31/1996	Krause et al.	
	A26	5,625,626	04/29/1997	Umekita	
	A27	5,629,984	05/13/1997	McManis	
	A28	5,654,695	08/05/1997	Olnowich et al	
	A29	5,682,480	10/28/1997	Nakagawa	
	A30	5,689,566	11/18/1997	Nguyen	
	A31	5,689,641	11/18/1997	Ludwig et al.	
	A32	5,740,375	04/14/1998	Dunne et al.	
	A33	5,757,925	05/1998	Faybishenko	
	A34	5,764,906	06/1998	Edelstein et al.	
	A35	5,771,239	06/23/1998	Moroney et al.	
	A36	5,774,660	6/30/1998	Brendel et al	
	A37	5,787,172	07/28/1998	Arnold	
	A38	5,790,548	08/04/1998	Sitaraman et al.	
	A39	5,796,942	08/18/1998	Esbensen	
	A40	5,805,801	09/08/1998	Holloway et al.	
	A41	5,805,803	09/08/1998	Birrell et al.	
	A42	5,822,434	10/13/1998	Caronni et al.	
	A43	5,842,040	11/24/1998	Hughes et al.	
	A44	5,845,091	12/01/1998	Dunne et al.	
	A45	5,864,666	01/1999	Shrader, Theodore Jack London	
	A46	5,867,650	02/02/1998	Osterman	
	A47	5,870,610	02/09/1999	Beyda et al.	
	A48	5,878,231	05/02/1999	Baehr et al	
	A49	5,892,903	04/06/1999	Klaus	
	A50	5,898,830	04/27/1999	Wesinger, Jr. et al.	
	A51	5,905,859	05/18/1999	Holloway et al.	

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	**13/615,557**
	Filing Dates	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication/Patent Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A52	5,918,018	06/29/1999	Gooderum et al.	
	A53	5,918,019	06/29/1999	Valencia	
	A54	5,950,195	09/07/1999	Stockwell et al.	
	A55	5,950,519	09/14/1999	Anatoli	
	A56	5,960,204	09/28/1999	Yinger et al.	
	A57	5,996,016	11/30/1999	Thalheimer et al.	
	A58	6,006,259	12/21/1999	Adelman et al.	
	A59	6,006,272	12/21/1999	Aravamudan et al	
	A60	6,016,318	01/18/2000	Tomoike	
	A61	6,016,512	01/18/2000	Huitema	
	A62	6,041,342	03/21/2000	Yamaguchi	
	A63	6,052,788	04/2000	Wesinger et al.	
	A64	6,055,574	04/25/2000	Smorodinsky et al.	
	A65	6,061,346	05/2000	Nordman, Mikael	
	A66	6,061,736	05/09/2000	Rochberger et al	
	A67	6,079,020	06/20/2000	Liu	
	A68	6,081,900	06/2000	Subramaniam et al.	
	A69	6,092,200	07/18/2000	Muniyappa et al.	
	A70	6,101,182	08/2000	Sistanizadeh et al.	
	A71	6,119,171	09/12/2000	Alkhatib	
	A72	6,119,234	09/12/2000	Aziz et al.	
	A73	6,131,121	10/10/2000	Mattaway et al.	
	A74	6,147,976	11/14/2000	Shand et al.	
	A75	6,157,957	12/05/2000	Berthaud	
	A76	6,158,011	12/05/2000	Chen et al.	
	A77	6,168,409	01/02/2001	Fare	
	A78	6,173,399	01/09/2001	Gilbrech	
	A79	6,175,867	01/16/2001	Taghadoss	
	A80	6,178,409	01/23/2001	Weber et al.	
	A81	6,178,505	01/23/2001	Schneider et al	
	A82	6,179,102	01/30/2001	Weber, et al.	
	A83	6,182,141	1/30/2001	Blum et al.	
	A84	6,199,112	03/2001	Wilson, Stephen K.	
	A85	6,202,081	03/2001	Naudus, Stanley T.	
	A86	6,222,842	04/24/2001	Sasyan et al.	
	A87	6,223,287	04/24/2001	Douglas et al.	
	A88	6,226,748	05/01/2001	Bots et al.	
	A89	6,226,751	05/01/2001	Arrow et al..	
	A90	6,233,618	05/15/2001	Shannon	
	A91	6,243,360	06/05/2001	Basilico	
	A92	6,243,749	06/05/2001	Sitaraman et al.	
	A93	6,243,754	06/05/2001	Guerin et al	
	A94	6,246,670	06/12/2001	Karlsson et al.	
	A95	6,256,671	07/03/2001	Strentzsch et al.	
	A96	6,262,987	07/17/01	Mogul, Jeffrey C.	
	A97	6,263,445	07/17/2001	Blumenau	
	A98	6,269,099	07/31/2001	Borella et al.	
	A99	6,286,047	09/04/2001	Ramanathan et al	
	A100	6,298,341	10/02/01	Mann, et al.	
	A101	6,301,223	10/9/2001	Hrastar et al	
	A102	6,308,213	10/23/2001	Valencia	
	A103	6,308,274	10/23/2001	Swift	

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	**13/615,557**
	Filing Dates	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication/Patent Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A104	6,311,207	10/30/2001	Mighdoll et al	
	A105	6,314,463	11/2001	Abbott et al.	
	A106	6,324,161	11/27/2001	Kirch	
	A107	6,330,562	12/11/2001	Boden et al.	
	A108	6,332,158	12/18/2001	Risley et al.	
	A109	6,333,272	12/25/01	McMillin, et al.	
	A110	6,338,082	01/08/02	Schneider, Eric	
	A111	6,353,614	03/05/2002	Borella et al.	
	A112	6,425,003	07/23/2002	Herzog et al.	
	A113	6,430,155	08/06/2002	Davie et al	
	A114	6,430,610	08/06/2002	Carter	
	A115	6,487,598	11/26/2002	Valencia	
	A116	6,496,867	12/17/2002	Beser et al.	
	A117	6,499,108	12/24/2002	Johnson	
	A118	6,502,135	12/2002	Munger et al.	
	A119	6,505,232	01/07/2003	Mighdoll et al	
	A120	6,510,154	01/21/2003	Mayes et al	
	A121	6,549,516	04/15/2003	Albert et al	
	A122	6,557,037	04/2003	Provino, Joseph E.	
	A123	6,560,634	05/06/2003	Broadhurst	
	A124	6,571,296	05/27/2002	Dillon	
	A125	6,571,338	05/27/2003	Shaio et al.	
	A126	6,581,166	7/17/2003	Hirst et al.	
	A127	6,606,708	08/12/2003	Devine et al.	
	A128	6,615,357	9/2/2003	Boden et al.	
	A129	6,618,761	09/09/2003	Munger et al.	
	A130	6,671,702	12/30/2003	Kruglikov et al	
	A131	6,687,551	2/3/2004	Steindl	
	A132	6,687,746	02/03/04	Shuster, et al.	
	A133	6,701,437	03/02/2004	Hoke et al.	
	A134	6,714,970	3/30/2004	Fiveash et al.	
	A135	6,717,949	4/6/2004	Boden et al.	
	A136	6,751,738	06/15/2004	Wesinger, Jr. et al..	
	A137	6,752,166	06/22/04	Lull, et al.	
	A138	6,757,740	06/29/04	Parekh, et al.	
	A139	6,760,766	7/6/2004	Sahlqvist	
	A140	6,813,777	11/2004	Weinberger et al.	
	A141	6,826,616	11/30/2004	Larson et al.	
	A142	6,839,759	1/4/2005	Larson et al.	
	A143	6,937,597	08/30/2005	Rosenberg et al.	
	A144	7,010,604	3/7/2006	Munger et al.	
	A145	7,039,713	05/2006	Van Gunter et al.	
	A146	7,072,964	07/04/2006	Whittle et al.	
	A147	7,133,930	11/7/2006	Munger et al.	
	A148	7,167,904	01/23/07	Devarajan, et al.	
	A149	7,188,175	03/06/07	McKeeth, James A.	
	A150	7,188,180	3/6/2007	Larson et al.	
	A151	7,197,563	3/27/2007	Sheymov et al.	
	A152	7,353,841	04/08/08	Kono, et al.	
	A153	7,418,504	08/2008	Larson et al.	
	A154	7,461,334	12/02/08	Lu, et al.	
	A155	7,490,151	02/2009	Munger et al.	

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	**13/615,557**
	Filing Dates	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication/Patent Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A156	7,493,403	02/2009	Shull et al.	
	A157	7,584,500	09/2009	Dillon et al.	
	A158	7,764,231	07/27/2010	Karr et al.	
	A159	7,852,861	12/2010	Wu et al.	
	A160	7,921,211	04/2011	Larson et al.	
	A161	7,933,990	04/2011	Munger et al.	
	A162	8,051,181	11/2011	Larson et al.	

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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

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.	

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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

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	Translation 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			
	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			

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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

		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.	
	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.	

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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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	I. 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)	

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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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)	
	D52	Aventail Corp., "Managing Corporate Access to the Internet," Aventail AutoSOCKS White Paper *available at* http://web.archive.org/19970620030312/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)	

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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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)	
	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)	

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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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)	
	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)	

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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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)	
	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)	

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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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)	
	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	

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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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)	
	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)	

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	13/615,557
Filing Date	September 13, 2012
First Named Inventor	Victor Larson
Art Unit	2431
Examiner Name	Not Yet Assigned
Docket Number	77580-177 (VRNK-0001CP3CON8)

	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)	
	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)	

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	**13/615,557**
Filing Date	**September 13, 2012**
First Named Inventor	**Victor Larson**
Art Unit	**2431**
Examiner Name	**Not Yet Assigned**
Docket Number	**77580-177 (VRNK-0001CP3CON8)**

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)
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," 9 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)

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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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	
	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 Intemet 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)	

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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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	
	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 vs. Claims of the '211 Patent	
	D316	Exhibit 2, IETF RFC 2065: Domain Name System Security Extensions; Published January 1997 vs. Claims of the '504 Patent	
	D317	Exhibit 3, RFC 2543 vs. Claims of the '135 Patent	
	D318	Exhibit 4, RFC 2543 vs. Claims of the '211 Patent	
	D319	Exhibit 5, RFC 2543 vs. Claims of the '504 Patent	
	D320	Exhibit 6, SIP Draft v.2 vs. Claims of the '135 Patent	
	D321	Exhibit 7, SIP Draft v.2 vs. Claims of the '211 Patent	
	D322	Exhibit 8, SIP Draft v.2 vs. Claims of the '504 Patent	
	D323	Exhibit 9, H.323 vs. Claims of the '135 Patent	
	D324	Exhibit 10, H.323 vs. Claims of the '211 Patent	
	D325	Exhibit 11, H.323 vs. Claims of the '504 Patent	
	D326	Exhibit 12, SSL 3.0 vs. Claims of the '135 Patent .	
	D327	Exhibit 13, SSL 3.0 vs. Claims of the '211 Patent	
	D328	Exhibit 14, SSL 3.0 vs. Claims of the '504 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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D329	Exhibit 15, RFC 2487 vs. Claims of the '135 Patent	
	D330	Exhibit 16, RFC 2487 vs. Claims of the '211 Patent	
	D331	Exhibit 17, RFC 2487 vs. Claims of the '504 Patent	
	D332	Exhibit 18, RFC 2595 vs. Claims of the '135 Patent	
	D333	Exhibit 19, RFC 2595 vs. Claims of the '211 Patent	
	D334	Exhibit 20, RFC 2595 vs. Claims of the '504 Patent	
	D335	Exhibit 21, iPass vs. Claims of the '135 Patent	
	D336	Exhibit 22, iPASS vs. Claims of the '211 Patent	
	D337	Exhibit 23, iPASS vs. Claims of the '504 Patent	
	D338	Exhibit 24, "US '034" vs. Claims of the '135 Patent	
	D339	Exhibit 25, US Patent No. 6,453,034 ("US '034") vs. Claims of the '211 Patent	
	D340	Exhibit 26, US Patent No. 6,453,034 ("US '034") vs. Claims of the '504 Patent	
	D341	Exhibit 27, US '287 vs. Claims of the '135 Patent	
	D342	Exhibit 28, US '287 vs. Claims of the '211 Patent	
	D343	Exhibit 29, US '287 vs. Claims of the '504 Patent	
	D344	Exhibit 30, Overview of Access VPNs vs. Claims of the '135 Patent	
	D345	Exhibit 31, Overview of Access VPNs vs. Claims of the '211 Patent	
	D346	Exhibit 32, Overview of Access VPNs vs. Claims of the '504 Patent	
	D347	Exhibit 34, RFC 1928 vs. Claims of the '135 Patent	
	D348	Exhibit 35, RFC 1928 vs. Claims of the '211 Patent	
	D349	Exhibit 36, RFC 1928 vs. Claims of the '504 Patent	
	D350	Exhibit 37, RFC 2661 vs. Claims of the '135 Patent	
	D351	Exhibit 38, RFC 2661 vs. Claims of the '211 Patent	
	D352	Exhibit 39, RFC 2661 vs. Claims of the '504 Patent	
	D353	Exhibit 40, SecureConnect vs. Claims of the '135 Patent	
	D354	Exhibit 41, SecureConnect vs. Claims of the '211 Patent	
	D355	Exhibit 42,SecureConnect vs. Claims of the '504 Patent	
	D356	Exhibit 43, SFS-HTTP vs. Claims of the '135 Patent	
	D357	Exhibit 44, SFS-HTTP vs. Claims of the '211 Patent	
	D358	Exhibit 45, SFS-HTTP vs. Claims of the '504 Patent	
	D359	Exhibit 46, US '883 vs. Claims of the '135 Patent	
	D360	Exhibit 47, US '883 vs. Claims of the '211 Patent	
	D361	Exhibit 48, US '883 vs. Claims of the '504 Patent	
	D362	Exhibit 49, US '132 vs. Claims of the '135 Patent	
	D363	Exhibit 50, US '132 vs. Claims of the '211 Patent	
	D364	Exhibit 51, US '132 vs. Claims of the '504 Patent	
	D365	Exhibit 52, US '213 vs. Claims of the '135 Patent	
	D366	Exhibit 53, US '213 vs. Claims of the '211 Patent	
	D367	Exhibit 54, US '213 vs. Claims of the '504 Patent	
	D368	Exhibit 55, B&M VPNs vs. Claims of the '135 Patent	
	D369	Exhibit 56, B&M VPNs vs. Claims of the '211 Patent	
	D370	Exhibit 57, B&M VPNs vs. Claims of the '504 Patent	
	D371	Exhibit 58, BorderManager vs. Claims of the '135 Patent	
	D372	Exhibit 59, BorderManager vs. Claims of the '211 Patent	
	D373	Exhibit 60, BorderManager vs. Claims of the '504 Patent	
	D374	Exhibit 61, Prestige 128 Plus vs. Claims of the '135 Patent	
	D375	Exhibit 62, Prestige 128 Plus vs. Claims of the '211 Patent	
	D376	Exhibit 63, Prestige 128 Plus vs. Claims of the '504 Patent	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

13615557 - GAU: 2453

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	**13/615,557**
Filing Date	**September 13, 2012**
First Named Inventor	**Victor Larson**
Art Unit	**2431**
Examiner Name	**Not Yet Assigned**
Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D377	Exhibit 64, RFC 2401 vs. Claims of the '135 Patent	
	D378	Exhibit 65, RFC 2401 vs. Claims of the '211 Patent	
	D379	Exhibit 66, RFC 2401 vs. Claims of the '504 Patent	
	D380	Exhibit 67, RFC 2486 vs. Claims of the '135 Patent	
	D381	Exhibit 68, RFC 2486 vs. Claims of the '211 Patent	
	D382	Exhibit 69, RFC 2486 vs. Claims of the '504 Patent	
	D383	Exhibit 70, Understanding IPSec vs. Claims of the '135 Patent	
	D384	Exhibit 71, Understanding IPSec vs. Claims of the '211 Patent	
	D385	Exhibit 72, Understanding IPSec vs. Claims of the '504 Patent	
	D386	Exhibit 73, US '820 vs. Claims of the '135 Patent	
	D387	Exhibit 74, US '820 vs. Claims of the '211 Patent	
	D388	Exhibit 75, US '820 vs. Claims of the '504 Patent	
	D389	Exhibit 76, US '019 vs. Claims of the '211 Patent	
	D390	Exhibit 77, US '019 vs. Claims of the '504 Patent	
	D391	Exhibit 78, US '049 vs. Claims of the '135 Patent	
	D392	Exhibit 79, US '049 vs. Claims of the '211 Patent	
	D393	Exhibit 80, US '049 vs. Claims of the '504 Patent	
	D394	Exhibit 81, US '748 vs. Claims of the '135 Patent	
	D395	Exhibit 82, US '261 vs. Claims of the '135 Patent	
	D396	Exhibit 83, US '261 vs. Claims of the '211 Patent	
	D397	Exhibit 84, US '261 vs. Claims of the '504 Patent	
	D398	Exhibit 85, US '900 vs. Claims of the '135 Patent	
	D399	Exhibit 86, US '900 vs. Claims of the '211 Patent	
	D400	Exhibit 87, US '900 vs. Claims of the '504 Patent	
	D401	Exhibit 88, US '671 vs. Claims of the '135 Patent	
	D402	Exhibit 89, US '671 vs. Claims of the '211 Patent	
	D403	Exhibit 90, US '671 vs. Claims of the '504 Patent	
	D404	Exhibit 91, JP '704 vs. Claims of the '135 Patent	
	D405	Exhibit 92, JP '704 vs. Claims of the '211 Patent	
	D406	Exhibit 93, JP '704 vs. Claims of the '504 Patent	
	D407	Exhibit 94, GB '841 vs. Claims of the '135 Patent	
	D408	Exhibit 95, GB '841 vs. Claims of the '211 Patent	
	D409	Exhibit 96, GB '841 vs. Claims of the '504 Patent	
	D410	Exhibit 97, US '318 vs. Claims of the '135 Patent	
	D411	Exhibit 98, US '318 vs. Claims of the '211 Patent	
	D412	Exhibit 99, US '318 vs. Claims of the '504 Patent	
	D413	Exhibit 100, VPN/VLAN vs. Claims of the '135 Patent	
	D414	Exhibit 101, Nikkei vs. Claims of the '135 Patent	
	D415	Exhibit 102, NIKKEI vs. Claims of the '211 Patent	
	D416	Exhibit 103, NIKKEI vs. Claims of the '504 Patent	
	D417	Exhibit 104, Special Anthology vs. Claims of the '135 Patent	
	D418	Exhibit 105, Omron vs. Claims of the '135 Patent	
	D419	Exhibit 106, Gauntlet System vs. Claims of the '135 Patent	
	D420	Exhibit 107, Gauntlet System vs. Claims of the '151 Patent	
	D421	Exhibit 108, Gauntlet System vs. Claims of the '180 Patent	
	D422	Exhibit 109, Gauntlet System vs. Claims of the '211 Patent	
	D423	Exhibit 110, Gauntlet System vs. Claims of the '504 Patent	
	D424	Exhibit 111, Gauntlet System vs. Claims of the '759 Patent	

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	13/615,557
Filing Date	September 13, 2012
First Named Inventor	Victor Larson
Art Unit	2431
Examiner Name	Not Yet Assigned
Docket Number	77580-177 (VRNK-0001CP3CON8)

	D425	Exhibit 112, IntraPort System vs. Claims of the '135 Patent	
	D426	Exhibit 113, IntraPort System vs. Claims of the '151 Patent	
	D427	Exhibit 114, IntraPort System vs. Claims of the '180 Patent	
	D428	Exhibit 115, IntraPort System vs. Claims of the '211 Patent	
	D429	Exhibit 116, IntraPort System vs. Claims of the '504 Patent	
	D430	Exhibit 117, IntraPort System vs. Claims of the '759 Patent	
	D431	Exhibit 118, Altiga VPN System vs. Claims of the '135 Patent	
	D432	Exhibit 119, Altiga VPN System vs. Claims of the '151 Patent	
	D433	Exhibit 120, Altiga VPN System vs. Claims of the '180 Patent	
	D434	Exhibit 121, Altiga VPN System vs. Claims of the '211 Patent	
	D435	Exhibit 122, Altiga VPN System vs. Claims of the '504 Patent	
	D436	Exhibit 123, Altiga VPN System vs. Claims of the '759 Patent	
	D437	Exhibit 124, Kiuchi vs. Claims of the '135 Patent	
	D438	Exhibit 125, Kiuchi vs. Claims of the '151 Patent	
	D439	Exhibit 126, Kiuchi vs. Claims of the '180 Patent	
	D440	Exhibit 127, Kiuchi vs. Claims of the '211 Patent	
	D441	Exhibit 128, Kiuchi vs. Claims of the '504 Patent	
	D442	Exhibit 129, Kiuchi vs. Claims of the '759 Patent	
	D443	Exhibit 130, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '135 Patent	
	D444	Exhibit 131, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '151 Patent	
	D445	Exhibit 132, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '180 Patent	
	D446	Exhibit 133, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '211 Patent	
	D447	Exhibit 134, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '504 Patent	
	D448	Exhibit 135, Overview vs. Claims of the '759 Patent	
	D449	Exhibit 136, RFC 2401 vs. Claims of the '759 Patent	
	D450	Exhibit 137, Schulzrinne vs. Claims of the '135 Patent	
	D451	Exhibit 138, Schulzrinne vs. Claims of the '151 Patent	
	D452	Exhibit 139, Schulzrinne vs. Claims of the '180 Patent	
	D453	Exhibit 140, Schulzrinne vs. Claims of the '211 Patent	
	D454	Exhibit 141, Schulzrinne vs. Claims of the '504 Patent	
	D455	Exhibit 142, Schulzrinne vs. Claims of the '759 Patent	
	D456	Exhibit 143, Solana vs. Claims of the '135 Patent	
	D457	Exhibit 144, Solana vs. Claims of the '151 Patent	
	D458	Exhibit 145, Solana vs. Claims of the '180 Patent	
	D459	Exhibit 146, Solana vs. Claims of the '211 Patent	
	D460	Exhibit 147, Solana vs. Claims of the '504 Patent	
	D461	Exhibit 148, Solana vs. Claims of the '759 Patent	
	D462	Exhibit 149, Atkinson vs. Claims of the '135 Patent	
	D463	Exhibit 150, Atkinson vs. Claims of the '151 Patent	
	D464	Exhibit 151, Atkinson vs. Claims of the '180 Patent	
	D465	Exhibit 152, Atkinson vs. Claims of the '211 Patent	
	D466	Exhibit 153, Atkinson vs. Claims of the '504 Patent	
	D467	Exhibit 154, Atkinson vs. Claims of the '759 Patent	
	D468	Exhibit 155, Marino 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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D469	Exhibit 156, Marino vs. Claims of the '151 Patent	
	D470	Exhibit 157, Marino vs. Claims of the '180 Patent	
	D471	Exhibit 158, Marino vs. Claims of the '211 Patent	
	D472	Exhibit 159, Marino vs. Claims of the '504 Patent	
	D473	Exhibit 160, Marino vs. Claims of the '759 Patent	
	D474	Exhibit 161, Aziz ('646) vs. Claims of the '759 Patent	
	D475	Exhibit 162, Wesinger vs. Claims of the '135 Patent	
	D476	Exhibit 163, Wesinger vs. Claims of the '151 Patent	
	D477	Exhibit 164, Wesinger vs. Claims of the '180 Patent	
	D478	Exhibit 165, Wesinger vs. Claims of the '211 Patent	
	D479	Exhibit 166, Wesinger vs. Claims of the '504 Patent	
	D480	Exhibit 167, Wesinger vs. Claims of the '759 Patent	
	D481	Exhibit 168, Aziz ('234) vs. Claims of the '135 Patent	
	D482	Exhibit 169, Aziz ('234) vs. Claims of the '151 Patent	
	D483	Exhibit 170, Aziz ('234) vs. Claims of the '180 Patent	
	D484	Exhibit 171, Aziz ('234) vs. Claims of the '211 Patent	
	D485	Exhibit 172, Aziz ('234) vs. Claims of the '504 Patent	
	D486	Exhibit 173, Aziz ('234) vs. Claims of the '759 Patent	
	D487	Exhibit 174, Schneider vs. Claims of the '759 Patent	
	D488	Exhibit 175, Valencia vs. Claims of the '135 Patent	
	D489	Exhibit 176, Valencia vs. Claims of the '151 Patent	
	D490	Exhibit 177, Valencia vs. Claims of the '180 Patent	
	D491	Exhibit 178, Valencia vs. Claims of the '211 Patent	
	D492	Exhibit 179, Valencia vs. Claims of the '504 Patent	
	D493	Exhibit 180, RFC 2401 in Combination with U.S. Patent No. 6,496,867 vs. Claims of the '180 Patent	
	D494	Exhibit 181, Davison vs. Claims of the '135 Patent	
	D495	Exhibit 182, Davison vs. Claims of the '151 Patent	
	D496	Exhibit 183, Davison vs. Claims of the '180 Patent	
	D497	Exhibit 184, Davison vs. Claims of the '211 Patent	
	D498	Exhibit 185, Davison vs. Claims of the '504 Patent	
	D499	Exhibit 186, Davison vs. Claims of the '759 Patent	
	D500	Exhibit 187, AutoSOCKS v2.1 vs. Claims of the '135 Patent	
	D501	Exhibit 188, AutoSOCKS v2.1 vs. Claims of the '151 Patent	
	D502	Exhibit 189, AutoSOCKS v2.1 Administrator's Guide vs. Claims of the '180 Patent	
	D503	Exhibit 190, AutoSOCKS vs. Claims of the '759 Patent	
	D504	Exhibit 191, Aventail Connect 3.01/2.51 vs. Claims of the '135 Patent	
	D505	Exhibit 192, Aventail Connect v3.01/2.51 vs. Claims of the '151 Patent	
	D506	Exhibit 193, Aventail Connect 3.01/2.51 vs. Claims of the '180 Patent	
	D507	Exhibit 194, Aventail Connect 3.01/2.51 vs. Claims of the '759 Patent	
	D508	Exhibit 195, Aventail Connect 3.1/2.6 Administrator's Guide vs. Claims of the '135 Patent	
	D509	Exhibit 196, Aventail Connect 3.1/2.6 Administrator's Guide vs. Claims of the '151 Patent	
	D510	Exhibit 197, Aventail Connect 3.1/2.6 vs. Claims of the '180 Patent	
	D511	Exhibit 198, Aventail Connect 3.1/2.6 vs. Claims of the '759 Patent	
	D512	Exhibit 199, BinGO! User's User's Guide/Extended Features Reference vs. Claims of the '151 Patent	
	D513	Exhibit 200, BinGO! User's User's Guide/Extended Features Reference vs. Claims of the '135 Patent	
	D514	Exhibit 201, BinGO! vs. Claims of the '180 Patent	
	D515	Exhibit 202, BinGO! vs. Claims of the '759 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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D516	Exhibit 203, Broadband Forum Technical Report TR-025 (Issue 1.0/5.0) vs. Claims of the '135 Patent	
	D517	Exhibit 204, Domain Name System (DNS) Security vs. Claims of the '211 Patent	
	D518	Exhibit 205, Domain Name System (DNS) Security vs. Claims of the '504 Patent	
	D519	Exhibit 206, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '211 Patent	
	D520	Exhibit 207, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '504 Patent	
	D521	Exhibit 208, RFC 2538, Storing Certificates in the Domain Name System (DNS) vs. Claims of the '211 Patent	
	D522	Exhibit 209, RFC 2538, Storing Certificates in the Domain Name System (DNS) vs. Claims of the '504 Patent	
	D523	Exhibit 210, IETF RFC 2065: Domain Name System Security Extensions; Published January 1997 vs. Claims of the '504 Patent	
	D524	Exhibit 211, IETF RFC 2065: Domain Name System Security Extensions; Published January 1997 vs. Claims of the '211 Patent	
	D525	Exhibit 212, RFC 2486, RFC 2661, RFC 2401, and Internet-Draft, "Secure Remote Access with L2TP" vs. Claims of the '135 Patent	
	D526	Exhibit 213, U.S. Patent No. 7,100,195 in Combination with RFC 2401 and U.S. Patent No. 6,496,867 vs. Claims of the '135 Patent	
	D527	Exhibit 214, U.S. Patent No. 7,100,195 in Combination with RFC 2401 and U.S. Patent No. 6,496,867 vs. Claims of the '151 Patent	
	D528	Exhibit 215, U.S. Patent No. 6,643,701 vs. Claims of the '135 Patent	
	D529	Exhibit 216, U.S. Patent No. 6,643,701 vs. Claims of the '151 Patent	
	D530	Exhibit 217, U.S. Patent No. 6,496,867 in Combination with RFC 2401 vs. Claims of the '151 Patent	
	D531	Exhibit 218, U.S. Patent No. 6,496,867 in Combination with RFC 2401 vs. Claims of the '135 Patent	
	D532	Exhibit 219, U.S. Patent No. 6,496,867 vs. Claims of the '211 Patent	
	D533	Exhibit 220, U.S. Patent No. 6,496,867 vs. Claims of the '504 Patent	
	D534	Exhibit 221, RFC 2486, RFC 2661, RFC 2401, and Internet-Draft, "Secure Remote Access with L2TP" vs. Claims of the '151 Patent	
	D535	Exhibit 222, U.S. Patent No. 6,557,037 vs. Claims of the '211 Patent	
	D536	Exhibit 223, U.S. Patent No. 6,557,037 vs. Claims of the '504 Patent	
	D537	Exhibit 224, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '135 Patent	
	D538	Exhibit 225, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '151 Patent	
	D539	Exhibit Cisco-1, Cisco's Prior Art Systems vs. Claims of the '135 Patent	
	D540	Exhibit Cisco-2, Cisco's Prior Art Systems vs. Claims of the '151 Patent	
	D541	Exhibit Cisco-3, Cisco's Prior Art Systems vs. Claims of the '180 Patent	
	D542	Exhibit Cisco-4, Cisco's Prior Art Systems vs. Claims of the '211 Patent	
	D543	Exhibit Cisco-5, Cisco's Prior Art Systems vs. Claims of the '504 Patent	
	D544	Exhibit Cisco-6, Cisco's Prior Art Systems vs. Claims of the '759 Patent	
	D545	Exhibit Cisco-7, Cisco's Prior Art PIX System vs. Claims of the '759 Patent	
	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)	

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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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 *VirnetX 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).	
	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).	

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	**13/615,557**
Filing Date	**September 13, 2012**
First Named Inventor	**Victor Larson**
Art Unit	**2431**
Examiner Name	**Not Yet Assigned**
Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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").	
	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: Simpson, 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)	

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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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	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	
	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 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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D660	Exhibit 38, RFC 2661 vs. Claims of the '211 Patent	
	D661	Exhibit 39, RFC 2661 vs. Claims of the '504 Patent	
	D662	Exhibit 40, SecureConnect vs. Claims of the '135 Patent	
	D663	Exhibit 41, SecureConnect vs. Claims of the '211 Patent	
	D664	Exhibit 42, SecureConnect vs. Claims of the '504 Patent	
	D665	Exhibit 43, SFS-HTTP vs. Claims of the '135 Patent	
	D666	Exhibit 44, SFS-HTTP vs. Claims of the '211 Patent	
	D667	Exhibit 45, SFS-HTTP vs. Claims of the '504 Patent	
	D668	Exhibit 46, US '883 vs. Claims of the '135 Patent	
	D669	Exhibit 47, US '883 vs. Claims of the '211 Patent	
	D670	Exhibit 48, US '883 vs. Claims of the '504 Patent	
	D671	Exhibit 49, Chuah vs. Claims of the '135 Patent	
	D672	Exhibit 50, Chuah vs. Claims of the '211 Patent	
	D673	Exhibit 51, Chuah vs. Claims of the '504 Patent	
	D674	Exhibit 52, U.S. '648 vs. Claims of the '135 Patent	
	D675	Exhibit 53, U.S. '648 vs. Claims of the '211 Patent	
	D676	Exhibit 57, B&M VPNs vs. Claims of the '504 Patent	
	D677	Exhibit 58, BorderManager vs. Claims of the '135 Patent	
	D678	Exhibit 59, BorderManager vs. Claims of the '211 Patent	
	D679	Exhibit 60, BorderManager vs. Claims of the '504 Patent	
	D680	Exhibit 61, Prestige 128 Plus vs. Claims of the '135 Patent	
	D681	Exhibit 62, Prestige 128 Plus vs. Claims of the '211 Patent	
	D682	Exhibit 63, Prestige 128 Plus vs. Claims of the '504 Patent	
	D683	Exhibit 64, RFC 2401 vs. Claims of the '135 Patent	
	D684	Exhibit 65, RFC 2401 vs. Claims of the '211 Patent	
	D685	Exhibit 66, RFC 2401 vs. Claims of the '504 Patent	
	D686	Exhibit 67, US '072 vs. Claims of the '135 Patent	
	D687	Exhibit 68, RFC 2486 vs. Claims of the '211 Patent	
	D688	Exhibit 69, RFC 2486 vs. Claims of the '504 Patent	
	D689	Exhibit 70 Understanding IPSec vs. Claims of the '135 Patent	
	D690	Exhibit 71, Understanding IPSec vs. Claims of the '211 Patent	
	D691	Exhibit 72, Understanding IPSec vs. Claims of the '504 Patent	
	D692	Exhibit 73, US '820 vs. Claims of the '135 Patent	
	D693	Exhibit 74, US '820 vs. Claims of the '211 Patent	
	D694	Exhibit 75, US '820 vs. Claims of the '504 Patent	
	D695	Exhibit 76, US '019 vs. Claims of the '211 Patent	
	D696	Exhibit 77, US '019 vs. Claims of the '504 Patent	
	D697	Exhibit 78, US '049 vs. Claims of the '135 Patent	
	D698	Exhibit 79, US '049 vs. Claims of the '211 Patent	
	D699	Exhibit 80, US '049 vs. Claims of the '504 Patent	
	D700	Exhibit 81, US '748 vs. Claims of the '135 Patent	
	D701	Exhibit 82, US '261 vs. Claims of the '135 Patent	
	D702	Exhibit 83, US '261 vs. Claims of the '211 Patent	
	D703	Exhibit 84, US '261 vs. Claims of the '504 Patent	
	D704	Exhibit 85, US '900 vs. Claims of the '135 Patent	
	D705	Exhibit 86, US '900 vs. Claims of the '211 Patent	
	D706	Exhibit 87, US '900 vs. Claims of the '504 Patent	
	D707	Exhibit 88, US '671 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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D708	Exhibit 89, US '671 vs. Claims of the '211 Patent	
	D709	Exhibit 90, US '671 vs. Claims of the '504 Patent	
	D710	Exhibit 91, JP '704 vs. Claims of the '135 Patent	
	D711	Exhibit 92, JP '704 vs. Claims of the '211 Patent	
	D712	Exhibit 93, JP '704 vs. Claims of the '504 Patent	
	D713	Exhibit 94, GB '841 vs. Claims of the '135 Patent	
	D714	Exhibit 95, GB '841 vs. Claims of the '211 Patent	
	D715	Exhibit 96, GB '841 vs. Claims of the '504 Patent	
	D716	Exhibit 97, US '318 vs. Claims of the '135 Patent	
	D717	Exhibit 98, US '318 vs. Claims of the '211 Patent	
	D718	Exhibit 99, US '318 vs. Claims of the '504 Patent	
	D719	Exhibit 100, VPN/VLAN vs. Claims of the '135 Patent	
	D720	Exhibit 101, Nikkei vs. Claims of the '135 Patent	
	D721	Exhibit 102, Nikkei vs. Claims of the '211 Patent	
	D722	Exhibit 103, Nikkei vs. Claims of the '504 Patent	
	D723	Exhibit 104, Special Anthology vs. Claims of the '135 Patent	
	D724	Exhibit 106-A, Gauntlet System vs. Claims of the '135 Patent	
	D725	Exhibit 109-A, Gauntlet System vs. Claims of the '211 Patent	
	D726	Exhibit 110-A, Gauntlet System vs. Claims of the '504 Patent	
	D727	Exhibit 112, IntraPort System vs. Claims of the '135 Patent	
	D728	Exhibit 115, IntraPort System vs. Claims of the '211 Patent	
	D729	Exhibit 116, IntraPort System vs. Claims of the '504 Patent	
	D730	Exhibit 118, Altiga VPN System vs. Claims of the '135 Patent	
	D731	Exhibit 121, Altiga VPN System vs. Claims of the '211 Patent	
	D732	Exhibit 122, Altiga VPN System vs. Claims of the '504 Patent	
	D733	Exhibit 124, Kiuchi vs. Claims of the '135 Patent	
	D734	Exhibit 127, Kiuchi vs. Claims of the '211 Patent	
	D735	Exhibit 128, Kiuchi vs. Claims of the '504 Patent	
	D736	Exhibit 137, Schulzrinne vs. Claims of the '135 Patent	
	D737	Exhibit 137, Schulzrinne vs. Claims of the '135 (Final) Patent	
	D738	Exhibit 140, Schulzrinne vs. Claims of the '211 Patent	
	D739	Exhibit 141, Schulzrinne vs. Claims of the '504 Patent	
	D740	Exhibit 143, Solana vs. Claims of the '135 Patent	
	D741	Exhibit 146, Solana vs. Claims of the '211 Patent	
	D742	Exhibit 147, Solana vs. Claims of the '504 Patent	
	D743	Exhibit 155, Marino vs. Claims of the '135 Patent	
	D744	Exhibit 158, Marino vs. Claims of the '211 Patent	
	D745	Exhibit 159, Marino vs. Claims of the '504 Patent	
	D746	Exhibit 168, Aziz vs. Claims of the '135 Patent	
	D747	Exhibit 171, U.S. '234 vs. Claims of the '211 Patent	
	D748	Exhibit 172, Aziz vs. Claims of the '504 Patent	
	D749	Exhibit 175, Valencia vs. Claims of the '135 Patent	
	D750	Exhibit 178, Valencia vs. Claims of the '211 Patent	
	D751	Exhibit 179, Valencia vs. Claims of the '504 Patent	
	D752	Exhibit 181, Davison vs. Claims of the '135 Patent	
	D753	Exhibit 184, Davison vs. Claims of the '211 Patent	
	D754	Exhibit 185, Davison vs. Claims of the '504 Patent	
	D755	Exhibit 200, BinGO! User's Guide/Extended Features Reference 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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D756	Exhibit 203, Broadband Forum Technical Report TR-025 (Issue 1.0/5.0) vs. Claims of the '135 Patent	
	D757	Exhibit 206, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '211 Patent	
	D758	Exhibit 207, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '504 Patent	
	D759	Exhibit 208, RFC 2538, Storing Certificates in the Domain Name System (DNS) vs. Claims of the '211 Patent	
	D760	Exhibit 209, RFC 2538, Storing Certificates in the Domain Name System (DNS) vs. Claims of the '504 Patent	
	D761	Exhibit 212, RFC 2486, RFC 2661, RFC 2401 and Internet-Draft, "Secure Remote Access with L2TP' vs. Claims of the '135 Patent	
	D762	Exhibit 218, U.S. Patent No. 6,496,867 in combination with RFC 2401' vs. Claims of the '135 Patent	
	D763	Exhibit 219, U.S. Patent No. 6,496,867 vs. Claims of the '211 Patent	
	D764	Exhibit 220, U.S. Patent No. 6,496,867 vs. Claims of the '504 Patent	
	D765	Exhibit 222, U.S. Patent No. 6,557,037 vs. Claims of the '211 Patent	
	D766	Exhibit 223, U.S. Patent No. 6,557,037 vs. Claims of the '504 Patent	
	D767	Exhibit 224, RFC 2230, Key Exchange Delegation Record for the DNS vs. Claims of the '135 Patent	
	D768	Exhibit 228, U.S. 588 vs. Claims of the '211 Patent (Final)	
	D769	Exhibit 229, U.S. 588 vs. Claims of the '504 Patent (Final)	
	D770	Exhibit 230, Microsoft VPN vs. Claims of the '135 Patent (Final)	
	D771	Exhibit 231, Microsoft VPN vs. Claims of the '211 Patent (Final)	
	D772	Exhibit XX, Microsoft VPN vs. Claims of the '504 Patent	
	D773	Exhibit Cisco-1, Cisco's Prior Art System vs. Claims of the '135 Patent	
	D774	Exhibit Cisco-4, Cisco's Prior Art System vs. Claims of the '211 Patent	
	D775	Exhibit Cisco-5, Cisco's Prior Art System vs. Claims of the '504 Patent	
	D776	Exhibit 225, US '037 vs. Claims of the '135 Patent	
	D777	Exhibit 226, ITU-T Standardization Activities vs. Claims of the '135 Patent	
	D778	Exhibit 227, US '393 vs. Claims of the '135 Patent	
	D779	Exhibit 233, The Miller Application vs. Claim 13 of the '135 Patent	
	D780	Exhibit 234, Aventail Connect 3.1/2.6 Administrator's Guide ("Aventail Connect") vs. Claims of the '504 Patent	
	D781	Exhibit 235, Microsoft VPN vs. Claims of the '504 Patent	
	D782	Exhibit 1, IETF RFC 2065: Domain Name System Security Extensions; published January 1997 vs. Claims of the '211 Patent	
	D783	Exhibit 2, IETF RFC 2065: Domain Name System Security Extensions; published January 1997 vs. Claims of the '504 Patent	
	D784	Exhibit 3, RFC 2543 vs. Claims of the '135 Patent	
	D785	Exhibit 4, RFC 2543 vs. Claims of the '211 Patent	
	D786	Exhibit 5, RFC 2543 vs. Claims of the '504 Patent	
	D787	Exhibit 6, SIP Draft v.2 vs. Claims of the '135 Patent	
	D788	Exhibit 7, SIP Draft v.2 vs. Claims of the '211 Patent	
	D789	Exhibit 8, SIP Draft v.2 vs. Claims of the '504 Patent	
	D790	Exhibit 9, H.323 vs. Claims of the '135 Patent	
	D791	Exhibit 10, H.323 vs. Claims of the '211 Patent	
	D792	Exhibit 11, H.323 vs. Claims of the '504 Patent	
	D793	Exhibit 12, SSL 3.0 vs. Claims of the '135 Patent	
	D794	Exhibit 13, SSL 3.0 vs. Claims of the '211 Patent	
	D795	Exhibit 14, SSL 3.0 vs. Claims of the '504 Patent	
	D796	Exhibit 15, RFC 2487 vs. Claims of the '135 Patent	
	D797	Exhibit 16, RFC 2487 vs. Claims of the '211 Patent	
	D798	Exhibit 17, RFC 2487 vs. Claims of the '504 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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D799	Exhibit 18, RFC 2595 vs. Claims of the '135 Patent	
	D800	Exhibit 21, iPass vs. Claims of the '135 Patent	
	D801	Exhibit 22, iPass vs. Claims of the '211 Patent	
	D802	Exhibit 23, iPass vs. Claims of the '504 Patent	
	D803	Exhibit 24, U.S. Patent No. 6,453,034 ('034 Patent") vs. Claims of the 135 Patent	
	D804	Exhibit 25, U.S. Patent No. 6,453,034 ('034 Patent") vs. Claims of the 211 Patent	
	D805	Exhibit 26, U.S. Patent No. 6,453,034 ('034 Patent") vs. Claims of the 504 Patent	
	D806	Exhibit 27, U.S. Patent No. 6,223,287 ("287 Patent") vs. Claims of the 135 Patent	
	D807	Exhibit 28, U.S. Patent No. 6,223,287 ("287 Patent") vs. Claims of the 211 Patent	
	D808	Exhibit 29, U.S. Patent No. 6,223,287 ("287 Patent") vs. Claims of the 504 Patent	
	D809	Exhibit 35, RFC 1928 vs. Claims of the '211 Patent	
	D810	Exhibit 36, RFC 1928 vs. Claims of the '504 Patent	
	D811	Exhibit 106, Gaunlet System and Gaunlet References vs. Claims of the '135 Patent	
	D812	Exhibit 109, Gaunlet System and Gaunlet References vs. Claims of the '211 Patent	
	D813	Exhibit 110, Gaunlet System vs. Claims of the '504 Patent	
	D814	Exhibit 130, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '135 Patent	
	D815	Exhibit 133, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '211 Patent	
	D816	Exhibit 134, Overview of Access VPNs and Tunneling Technologies ("Overview") vs. Claims of the '504 Patent	
	D817	Exhibit 149, Atkinson vs. Claims of the '135 Patent	
	D818	Exhibit 152, Atkinson vs. Claims of the '211 Patent	
	D819	Exhibit 153, Atkinson vs. Claims of the '504 Patent	
	D820	Exhibit 162, Wesinger vs. Claims of the '135 Patent	
	D821	Exhibit 165, Wesinger vs. Claims of the '211 Patent	
	D822	Exhibit 166, Wesinger vs. Claims of the '504 Patent	
	D823	Exhibit 187, AutoSOCKS v2.1 vs. Claims of the '135 Patent	
	D824	Exhibit 191, Aventail Connect 3.01/2.51 ("Aventail Connect") vs. Claims of the '135 Patent	
	D825	Exhibit 195, Aventail Connect 3.1/2.6 Administrator's Guide ("Aventail Connect") vs. Claims of the '135 Patent	
	D826	Exhibit 204, Domain Name System (DNS) Security vs. Claims of the '211 Patent	
	D827	Exhibit 205, Domain Name System (DNS) Security ("DNS Security") vs. Claims of the '504 Patent	
	D828	Exhibit 210, Lendenmann vs. Claims of the '211 Patent	
	D829	Exhibit 211, Lendenmann vs. Claims of the '504 Patent	
	D830	Exhibit 213, U.S. Patent No. 7,100,195 in combination with RFC 2401 and U.S. Patent No. 6,496,867 vs. Claims of the '135 Patent	
	D831	Exhibit 215, Aziz vs. Claims of the '135 Patent	
	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)	

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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D840	Exhibit D7, "Schimpf"; Brian C. Schimpf, "Securing Web Access with DCE," Presented at Network and Distributed System Security (Feb. 10-11, 1997)	
	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"	
	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").	

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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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 *VirnetX, 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	
	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	

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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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	
	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 vs. Claims of the '135 Patent	
	D911	Exhibit 227, Securing Web Access with DCE vs. Claims of the '151 Patent	
	D912	Exhibit 228, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '135 Patent	
	D913	Exhibit 229, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '151 Patent	
	D914	Exhibit 230, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '180 Patent	
	D915	Exhibit 231, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '211 Patent	
	D916	Exhibit 232, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '504 Patent	
	D917	Exhibit 233, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '759 Patent	
	D918	Exhibit 234, U.S. '648 vs. Claims of the '135 Patent	
	D919	Exhibit 235, U.S. '648 vs. Claims of the '211 Patent	
	D920	Exhibit 236, U.S. '648 vs. Claims of the '504 Patent	
	D921	Exhibit 237, U.S. '648 vs. Claims of the '135 Patent	
	D922	Exhibit 238, Gauntlet System vs. Claims of the '211 Patent	
	D923	Exhibit 239, Gauntlet System vs. Claims of the '504 Patent	
	D924	Exhibit 240, Gauntlet System vs. Claims of the '135 Patent	
	D925	Exhibit 241, U.S. '588 vs. Claims of the '211 Patent	
	D926	Exhibit 242, U.S. '588 vs. Claims of the '504 Patent	
	D927	Exhibit 243, Microsoft VPN vs. Claims of the '135 Patent	
	D928	Exhibit 244, Microsoft VPN vs. Claims of the '211 Patent	
	D929	Exhibit 245, Microsoft VPN vs. Claims of the '504 Patent	
	D930	Exhibit 246, ITU-T Standardization Activities vs. Claims of the '135 Patent	
	D931	Exhibit 247, U.S. '393 vs. Claims of the '135 Patent	
	D932	Exhibit 248, The Miller Application vs. Claim 13 of the '135 Patent	
	D933	Exhibit 249, Gauntlet System vs. Claims of the '151 Patent	
	D934	Exhibit 250, ITU-T Standardization Activities vs. Claims of the '151 Patent	
	D935	Exhibit 251, U.S. Patent No. 5,940,393 vs. Claims of the '151 Patent	
	D936	Exhibit 252, Microsoft VPN vs. Claims of the '151 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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D937	Exhibit 253, U.S. Patent No.6,324,648 vs. Claims of the '151 Patent	
	D938	Exhibit 254, U.S. Patent No.6,857,072 vs. Claims of the '151 Patent	
	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	
	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	PTO Form 1449	
	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	

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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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	
	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	PTO Form 1449	
	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 *VimetX, 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	
	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	

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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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	
	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	PTO Form 1449	
	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	

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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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	
	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 vs. Claims of the '135 Patent	
	D1056	Exhibit 227, Securing Web Access with DCE vs. Claims of the '151 Patent	
	D1057	Exhibit 228, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '135 Patent	
	D1058	Exhibit 229, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '151 Patent	
	D1059	Exhibit 230, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '180 Patent	
	D1060	Exhibit 231, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '211 Patent	
	D1061	Exhibit 232, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '504 Patent	
	D1062	Exhibit 233, Understanding OSF DCE 1.1 for AIX and OS/2 vs. Claims of the '759 Patent	
	D1063	Exhibit 234, U.S. '648 vs. Claims of the '135 Patent	
	D1064	Exhibit 235, U.S. '648 vs. Claims of the '211 Patent	
	D1065	Exhibit 236, U.S. '648 vs. Claims of the '504 Patent	
	D1066	Exhibit 237, U.S. '072 vs. Claims of the '135 Patent	
	D1067	Exhibit 238, Gauntlet System vs. Claims of the '211 Patent	
	D1068	Exhibit 239, Gauntlet System vs. Claims of the '504 Patent	
	D1069	Exhibit 240, Gauntlet System vs. Claims of the '135 Patent	
	D1070	Exhibit 241, U.S. '588 vs. Claims of the '211 Patent	
	D1071	Exhibit 242, U.S. '588 vs. Claims of the '504 Patent	
	D1072	Exhibit 243, Microsoft VPN vs. Claims of the '135 Patent	
	D1073	Exhibit 244, Microsoft VPN vs. Claims of the '211 Patent	
	D1074	Exhibit 245, Microsoft VPN vs. Claims of the '504 Patent	
	D1075	Exhibit 246, ITU-T Standardization Activities vs. Claims of the '135 Patent	
	D1076	Exhibit 247, U.S. '393 vs. Claims of the '135 Patent	
	D1077	Exhibit 248, The Miller Application vs. Claim 13 of the '135 Patent	
	D1078	Exhibit 249, Gauntlet System vs. Claims of the '151 Patent	
	D1079	Exhibit 250, ITU-T Standardization Activities vs. Claims of the '151 Patent	
	D1080	Exhibit 251, U.S. Patent No. 5,940,393 vs. Claims of the '151 Patent	
	D1081	Exhibit 252, Microsoft VPN vs. Claims of the '151 Patent	
	D1082	Exhibit 253, U.S. Patent No.6,324,648 vs. Claims of the '151 Patent	

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	**13/615,557**
Filing Date	**September 13, 2012**
First Named Inventor	**Victor Larson**
Art Unit	**2431**
Examiner Name	**Not Yet Assigned**
Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1083	Exhibit 254, U.S. Patent No.6,857,072 vs. Claims of the '151 Patent	
	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	
	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)	
	D1112	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	
	D1113	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	
	D1114	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	
	D1115	ITU-T Recommendation H.245, "Infrastructure of Audiovisual Services – Communication Procedures. Control Protocol for Multimedia Communication," International Telecommunication Union, pages 1-280, February 1998	
	D1116	Request for Inter Partes Reexamination Under 35 U.S.C. § 311 (Patent No.8,051,181)	
	D1117	Transmittal Letters (Patent No.8,051,181)	
	D1118	Exhibit X5, Droms, R., RFC 2131, "Dynamic Host Configuration Protocol," 1987	

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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1119	Hopen Transcript dated April 11, 2012	
	D1120	VirnetX Claim Construction Opinion	
	D1121	Declaration of Angelos D. Keromytic, Ph.D.	
	D1122	Declaration of Dr. Robert Dunham Short III	
	D1123	Exhibit A-1, Verdict Form from VirnetX, Inc. v. Microsoft Corp., No. 6:07-CV-80 (E.D. Tex.)	
	D1124	Exhibit A-3, Declaration of Jason Nieh, Ph.D. (Control No. 95/001,269)	
	D1125	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	
	D1126	Exhibit B-1, Excerpt from Deposition of Defense FY 2000/2001 Biennial Budget Estimates, Feb. 1999	
	D1127	Exhibit B-2, Collection of Reports and Presentations on DARPA Projects	
	D1128	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	
	D1129	Joel Snyder, Living in Your Own Private Idaho, Network World (January 28, 1998) http://www.networkworld.com/intranet/0126review.html.	
	D1130	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	
	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. 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]	
	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]	

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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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	
	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	

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	**13/615,557**
Filing Date	**September 13, 2012**
First Named Inventor	**Victor Larson**
Art Unit	**2431**
Examiner Name	**Not Yet Assigned**
Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	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	
	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	
	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	
	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)	
	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	
	D1215	Alexander Invalidity Expert Report dtd May 22, 2012 with Exhibits	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

13615557 - GAU: 2453

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1216	Deposition of Peter Alexander dtd July 27, 2012	
	D1217	Cisco '151 Comments by Third Party Requester dtd August 17, 2012 with Exhibits	
	D1218	Cisco '151 Petition to Waive Page Limit Requirement for Third Party Comments dtd August August 17, 2012	
	D1219	Deposition of Stuart Stubblebine dtd August 22, 2012	
	D1220	Defendants' Motion For Reconsideration of the Construction of the Term "Secure Communication Link," 7 pages, June 2012	
	D1221	Green, "Cisco Leverages Altiga Technology for VPN's," 2 pages, 2000 http://www.crn.com/news/channel-programs/18807923/cisco-leverages-altiga-technology-for-vpns.htm	
	D1222	Altiga Networks Archived at http://web.archive.org/web/20000823023437/http:/www.altiga.com/products/ 1999 and Retrieved by the Wayback Machine	
	D1223	Kiuchi, "C-HTTP The Development of a Secure, Closed HTTP-Based Network on the Internet," Department of Epidemiology and Biostatistics, Faculty of Medicine, University of Tokyo, Japan	
	D1224	Lee et al., "Uniform Resource Locators (URL)," Network Working Group, RFC 1738, December 1994 (25 pages)	
	D1225	VPN 3000 Concentrator Series, User Guide; Release 2.5 July 2000 (489 pages)	
	D1226	VPN 3000 Concentrator Series, Getting Started; Release 2.5 July 2000 (122 pages)	
	D1227	Fratto, Altiga Concentrates on VPN Security (Hardware Review Evaluation), Network Computing, March 22, 1999 (2 pages)	
	D1228	Response to RFP: Altiga, Network World Fusion, May 10, 1999 (7 pages)	
	D1229	Altiga Proves Multi-Vendor Interoperability for Seamless VPN Deployment; VPN Workshop Marks Significant Development in the VPN Market, July 12, 1999 (2 pages)	
	D1230	Altiga VPN Concentrator Series (C50) Versus Nortel Networks Contivity Extranet Switch 4000 and 4500, VPN Tunneling competitive Evaluation, 1999 (6 pages)	
	D1231	VPN 3000 Client User Guide, Release 2.5, July 2000 (94 pages)	
	D1232	Digital Certificates Design Specification for Release 2.0, May 17, 1999 (21 pages)	
	D1233	Altiga IPSec Client Architecture, Revision 1.0, April 5, 1999 (34 pages)	
	D1234	Altiga IPSec Functional Specification, Revision 2.1, (17 pages)	
	D1235	Altiga Product Requirements, Revision 1.7, May 26, 1998 (17 pages)	
	D1236	Altiga Network Lists Feature Functional Specification, Revision 1.0, (7 pages)	
	D1237	Altiga Split Tunneling Functional/Design Specification, (15 pages)	
	D1238	Altiga Digital Certificate Support for IPSec Client V2.1 Functional Specification, August 12, 1999 (24 pages)	
	D1239	Altiga IPSec LAN to LAN Tunnel Autodiscovery Functional Specification, (5 pages)	
	D1240	Altiga Split Tunneling Testplan, Revision 1.0, (8 pages)	
	D1241	Altiga VPN Concentrator Getting Started, Revision 1, March 1999 (116 pages)	
	D1242	Altiga VPN Concentrator Getting Started, Version 2, June 1999 (102 pages)	
	D1243	Altiga VPN Concentrator Getting Started, Version 3, December 1999 (130 pages)	
	D1244	Altiga VPN Concentrator Getting Started, Version 4, March 2000 (138 pages)	
	D1245	Altiga VPN Concentrator User Guide, Revision 1, March 1999 (304 pages)	

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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1246	Altiga VPN Concentrator User Guide, Revision 1.1, March 1999 (304 pages)	
	D1247	Altiga VPN Concentrator User Guide, Version 3, June 1999 (478 pages)	
	D1248	Altiga VPN Concentrator User Guide, Version 4, December 1999 (472 pages)	
	D1249	Altiga VPN Concentrator User Guide, Version 5, March 2000 (606 pages)	
	D1250	Altiga VPN Client Installation and User Guide, Version 2, July 1999 (92 pages)	
	D1251	Altiga VPN Concentrator VPN Client Installation and User Guide, Version 3, December 1999 (113 pages)	
	D1252	Altiga VPN Concentrator VPN Client Installation and User Guide, Version 4, March 2000 (118 pages)	
	D1253	Altiga Networks VPN Concentrator and VPN Client, as well as their Public Demonstrations and Testing, are also Described in Marketing Materials and Publications (4 pages)	

All references with no date, there are no date provided. /K.L./

/Krisna Lim/ 07/24/2013

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	**13/615,557**
Filing Date	**September 13, 2012**
First Named Inventor	**Victor Larson**
Art Unit	**2431**
Examiner Name	**Not Yet Assigned**
Docket Number	**77580-177 (VRNK-0001CP3CON8)**

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.

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, 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 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.

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[X] 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.

[ ] 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: October 22, 2012

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery L.L.P.
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

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	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

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
	A170	6,434,600	08/13/2002	Waite et al.	
	A171	7,225,249	05/29/2007	Barry et al.	

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
	B23	US2002/0004826	01/10/2002	Waite et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3-Number4-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.	
	D1413	Notice of Allowance dated August 9, 2013 from Corresponding U.S. Application Number 13/474,397	
	D1414	Office Action dated August 19, 2013 from Corresponding U.S. Application Number 13/903,788	

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 **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

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 any required fees 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/

Date: September 30, 2013

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 45414536-1.077580.0177

Electronic Acknowledgement Receipt

EFS ID:	16990580
Application Number:	13615557
International Application Number:	
Confirmation Number:	1089
Title of Invention:	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:	077580-0177
Receipt Date:	30-SEP-2013
Filing Date:	13-SEP-2012
Time Stamp:	15:00:00
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)	177.pdf	124933 f0e27726a4e6205613ebdcef28d203a560168afa	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	NOA892from164.pdf	409716 2f3206bdf597c1747caacec3dcf4ed31ba6f82f0	no	9
Warnings:					
Information:					
3	Non Patent Literature	OAdated81913from195.pdf	893586 f952b4a4d2fc2493749c6ceffc35d9a8db3ad1a2	no	24
Warnings:					
Information:					
		Total Files Size (in bytes):	1428235		

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.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

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
	A172	6,011,579	01/04/2000	Newlin	
	A173	8,504,696	08/06/2013	Larson et al.	
	A174	8,504,697	08/06/2013	Larson et al.	
	A175	6,335,966	01/01/2002	Toyoda	
	A176	6,195,677	02/27/2001	Utsumi	
	A177	6,959,184	10/25/2005	Byers et al.	

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 Code3-Number4-Kind Code5 *(if known)*	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No
						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.	
	D1415	Office Action dated October 1, 2013 from Corresponding U.S. Patent Application Number 13/911,813 (077580-0197)	

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 **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**13/615,557**
				Filing Date	**09-13-2012**
				First Named Inventor	**Victor Larson**
				Art Unit	**2453**
				Examiner Name	**Krisna Lim**
				Docket Number	**77580-177 (VRNK-0001CP3CON8)**

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 any required fees 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/ Date: September 30, 2013

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 45488253-1.077580.0177

Electronic Acknowledgement Receipt

EFS ID:	17040648
Application Number:	13615557
International Application Number:	
Confirmation Number:	1089
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer.
Filer Authorized By:	
Attorney Docket Number:	077580-0177
Receipt Date:	04-OCT-2013
Filing Date:	13-SEP-2012
Time Stamp:	16:44:08
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)	177.pdf	121183 1bfb30b932f5fec82150e85e26f28cdf6e4ac94d	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	197officeactiondtd100113.pdf	541010 f580579d465e664f5d124fc7b816db70a54a33e6	no	14
Warnings:					
Information:					
Total Files Size (in bytes):			662193		

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	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

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
	A178	6,058,250	05/02/2000	Harwood et al.	

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 Code3 -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.	
	D1416	Office Action dated October 10, 2013 from Corresponding U.S. Patent Application Number 13/950,877 (077580-0198)	

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 **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

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 any required fees 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/

Date: October 16, 2013

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 45906357-1.077580.0177

Electronic Acknowledgement Receipt

EFS ID:	17139233
Application Number:	13615557
International Application Number:	
Confirmation Number:	1089
Title of Invention:	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:	077580-0177
Receipt Date:	16-OCT-2013
Filing Date:	13-SEP-2012
Time Stamp:	15:19:17
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)	177.pdf	54300 27fe8865ef9a2e342039779af1877cd52f93bafe	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	OAdtd101013from198.pdf	786611 d56153c9d55e745fc982c7e8ebe2743382f47380	no	22
Warnings:					
Information:					
		Total Files Size (in bytes):	840911		

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.: 077580-0177
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Victor Larson, *et al.*	:	
	:	
Serial No.: 13/615,557	:	Confirmation No. 1089
	:	
Filed: September 13, 2012	:	Group Art Unit: 2453
	:	
Customer Number: 23630		Examiner: Lim, Krisna

For: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

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

AMENDMENT

Dear Commissioner:

In response to the Office Action mailed from the United States Patent and Trademark Office on August 1, 2013, please enter and consider the following:

Claims begin on page 2 of this paper.

Remarks begin on page 7 of this paper.

AMENDMENTS TO THE CLAIMS

This listing of the claims will replace all prior versions and listings of claims in the application:

1. (Currently Amended) A method of transparently creating an encrypted communications channel between a client device and a target device, each device being configured to allow ~~audio video~~ secure data communications between the client device and the target device over the encrypted communications channel once the encrypted communications channel is created, the method comprising:

(1) ~~receiving~~ intercepting from the client device a request ~~for a network~~to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device;

(2) determining whether the request to look up the IP address transmitted in step (1) ~~is requesting access~~corresponds to a device that accepts an encrypted channel connection with the client device; and

(3) in response to determining, in step (2), that the ~~address~~ request to look up the IP address in step (2) ~~is requesting access~~corresponds to a device that accepts an encrypted communications channel connection with the client device, providing provisioning information required to initiate the creation of the encrypted communications channel between the client device and the target device such that the encrypted communications channel supports secure ~~audio/video~~data communications transmitted between the two devices, the client device being a device at which a user accesses the encrypted communications channel.

2. (Currently Amended) The method of claim 1, wherein providing the provisioning information required to initiate the encrypted communications channel is based on a determination that the target device is a device with which an encrypted communications channel can be established when the IP address request corresponds to a target device identified in an network address lookup.

3. (Canceled)

4. (Currently Amended) The method of claim 1, wherein the ~~address request includes~~domain name is a secure domain name.

5. (Original) The method of claim 1, wherein the encrypted communications channel is a broadband connection.

6. (Original) The method of claim 1, wherein the encrypted communications channel is an unmodulated transmission link.

7. (Currently Amended) The method of claim 1, wherein the encrypted communications channel is a ~~umodulated~~ modulated transmission link.

8. (Currently Amended) The method of claim 1, wherein the encrypted communications channel supports at least one of the following: FDM~~FTM~~, TDM and CDMA.

9. (Original) The method of claim 1, wherein the client device is a phone.

10. (Currently Amended) The method of claim 9, wherein providing the provisioning information required to initiate the encrypted communications channel is based on a determination that the target device is a device with which an encrypted communications channel can be established when the IP address request corresponds to a target device identified in an network address lookup.

11. (Canceled)

12. (Currently Amended) The method of claim 9, wherein the ~~address request includes~~domain name is a secure domain name.

13. (Canceled)

14. (Original) The method of claim 9, wherein the encrypted communications channel is an unmodulated transmission link.

15. (Original) The method of claim 9, wherein the encrypted communications channel is a modulated transmission link.

16. (Currently Amended) The method of claim 9, wherein the encrypted communications channel supports at least one of the following: ~~FTM~~FDM, TDM and CDMA.

17. (Currently Amended) The method of ~~claim 9~~claim 1, wherein the target device is a server.

18. (Currently Amended) The method of ~~claim 9~~claim 1, wherein the target device is a phone.

19. (Currently Amended) A system for transparently creating an encrypted communications channel between a client device and a target device, each device being configured to allow ~~audio video~~secure data communications therebetween over an encrypted communications channel once the encrypted communications channel is created, the system including a memory storing instructions, and a server configuration arranged to:

(1) ~~receive~~ intercept from the client device a request to look up an Internet Protcol (IP)~~for a network~~ address corresponding to a domain name associated with the target device;

(2) determine whether the request to look up the IP address transmitted in step (1) ~~is requesting access~~corresponds to a device that accepts an encrypted channel connection with the client device; and

(3) in response to determining, in step (2), that the request to look up the IP address ~~request in step (2) is requesting access~~corresponds to a device that accepts an encrypted communications channel connection with the client device, provide provisioning information required to initiate the creation of the encrypted communications channel between the client device and the target device such that the encrypted communications channel supports secure ~~audio/video~~ data communications transmitted between the two devices, the client device being a device at which a user accesses the encrypted communications channel.

20. (Currently Amended) A system according to claim 19, wherein the encrypted communications channel supports a plurality of services ~~comprising a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof~~.

21. (New) The system according to claim 19, wherein the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof.

22. (New) The system according to claim 21, wherein the plurality of other application programs comprises at least one of the following: e-mail, a word processing program, and telephony.

23. (New) The system according to claim 19, wherein the domain name is a secure domain name.

24. (New) The system according to claim 19, wherein the encrypted communications channel is a broadband connection.

25. (New) The system according to claim 19, wherein the encrypted communications channel is an unmodulated transmission link.

26. (New) The system according to claim 19, wherein the encrypted communications channel is a modulated transmission link.

27. (New) The system according to claim 19, wherein the encrypted communications channel supports at least one of the following: FDM, TDM and CDMA.

28. (New) The system according to claim 19, wherein the client device is a phone.

29. (New) The system according to claim 19, wherein the target device is a server.

30. (New) The system according to claim 19, wherein the target device is a phone.

31. (New) The system according to claim 19, wherein intercepting the request consists of the system receiving the request to determine whether the target device accepts an encrypted channel connection with the client device.

32. (New) The system according to claim 19, wherein intercepting the request occurs within another device that is separate from the client device.

33. (New) The method according to claim 1, wherein intercepting the request consists of receiving the request to determine whether the target device accepts an encrypted channel connection with the client device.

34. (New) The method according to claim 1, wherein the intercepting the request occurs within another device that is separate from the client device.

35. (New) The method according to claim 1, wherein the encrypted communications channel supports a plurality of services.

36. (New) The method according to claim 35, wherein the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof.

37. (New) The method according to claim 36, wherein the plurality of other application programs comprises at least one of the following: e-mail, a word processing program, and telephony.

REMARKS

After entry of the foregoing amendments, claims 1, 2, 4-10, and 12, 14-37 are pending in the application, with claims 1 and 19 being the independent claims. Claims 3, 11, 13 are canceled without prejudice or disclaimer of subject matter. Claims 1, 2, 4, 7, 8, 10, 12, and 16-20 are amended, and new dependent claims 21-37 are added. No new matter is believed to have been added herein.

Claim Rejection – Double Patenting

Claims 1-20 are rejected on the ground of nonstatutory obviousness-type double patenting over various claims of U.S. Patent Nos. 7,933,990 and 7,490,151, and claims 1-19 are rejected on the ground of nonstatutory obviousness-type double patenting over various claims of U.S. Patent No. 6,502,135. Without conceding the correctness of the double patenting rejections, Applicants respectfully request reconsideration and withdrawal of the double patenting rejections in view of the foregoing claim amendments. Additionally or in the alternative, Applicants request that the requirement to file a terminal disclaimer be held in abeyance until the claims are indicated to be otherwise allowable.

Claim Rejection – 35 U.S.C. § 103

Claims 1-20 are rejected under 35 U.S.C. § 103(a) over U.S. Patent No. 5,898,830 ("*Wesinger*"). Reconsideration and withdrawal of the § 103 rejections are respectfully requested in view of the following remarks.

As an initial matter, the analysis provided by the Office Action does not address the language of the claims. For example, regarding claim 1, the Office Action contends that *Wesinger* discloses "a memory configured and arranged to facilitate a connection . . . of the client device . . . with a target device . . . over a secure communication link created . . . based on (i) an address request generated by the client device . . . and (ii) a determination as a result of the address request that the target device is a device with which a secure communication link can be established." (Office Action at 4-5 (emphasis in original).) However, original claim 1 does not recite these features, or other features used to support the rejection. Since the Office Action has not addressed the claim language of original claim 1, the Office Action has not provided sufficient evidence to establish a *prima facie* case of obviousness with respect to original claim 1. Accordingly, the rejection of claim 1 is deficient.

Wesinger teaches a firewall system that is configured as two or more sets of virtual hosts, with DNS mappings between the virtual hosts and respective remote hosts to be accessed through network interfaces of the firewall. (*Wesinger* Abstract.) The virtual hosts and DNS mappings enable transparent communications through the firewall. Each firewall "selectively allows 'acceptable' computer transmissions to pass through it and disallows other non-acceptable computer transmissions." (*Id.* at 1:8-12.)

In *Wesinger*, "[w]hen a connection request is received, the firewall spawns a process, or execution thread, to create a virtual host VHn to handle that connection request." (*Id.* at 15:9-12.) "Each virtual host has a separate configuration sub-file (sub-database) C1, C2, etc., that may be derived from a master configuration file, or database, 510. The configuration sub-files are text files that may be used to enable or disable different functions for each virtual host, specify which connections and types of traffic will be allowed and which will be denied, etc." (*Id.* at 14:46-52.) "Also as part of the configuration file of each virtual host, an access rules database is provided governing access to and through the virtual host, i.e., which connections will be allowed and which connections will be denied." (*Id.* at 15:24-28.) The virtual host process in *Wesinger* uses the access rules database to "allow only a connection from a specified secure client." (*Id.* at 10:14-16.)

In addition to connection requests, which trigger the virtual host process, *Wesinger* also separately discusses processing of DNS requests:

> When client C tries to initiate a connection to host D using the name of D, DNS **<u>operates in the usual manner</u>** to propagate a name request to successive levels of the network until D is found. The DNS server for D returns the network address of D to a virtual host on 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* 9:16-24 (emphasis added).) Accordingly, when client C uses a name of D in a DNS request, C gets back an address for a virtual host of firewall 105, which faces C (*See* Fig. 1).

The presently-claimed subject matter is patentable over *Wesinger*'s approach, as discussed below. Independent claim 1 is a representative claim.

Without conceding the correctness of the rejection, independent claim 1 has been amended to recite, *inter alia*:

> a method of transparently creating an encrypted communications channel between a client device and a target device, each device being configured to allow secure data communications between the client device and the target device over the encrypted communications channel once the encrypted communications channel is created, the method comprising:
>
> > (1) intercepting from the client device a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device;
> >
> > (2) determining whether the request to look up the IP address transmitted in step (1) corresponds to a device that accepts an encrypted channel connection with the client device; and
> >
> > (3) in response to determining, in step (2), that the request to look up the IP address in step (2) corresponds to a device that accepts an encrypted communications channel connection with the client device, providing provisioning information required to initiate the creation of the encrypted communications channel between the client device and the target device such that the encrypted communications channel supports secure data communications transmitted between the two devices, the client device being a device at which a user accesses the encrypted communications channel.

With regard to claim 1, *Wesinger* is not seen to disclose or suggest the feature "(2) determining whether the request to look up the IP address transmitted in step (1) corresponds to a device that accepts an encrypted channel connection with the client device." (*See* Office Action at 4-5.) As discussed above, *Wesinger*'s virtual host process checks parameters of a requested connection to determine whether a given connection should be allowed or denied. But this process acts upon a <u>connection request</u> and is not a "determin[ation] whether the request to look up the IP address transmitted in step (1) corresponds to a device that accepts an encrypted channel connection with the client device," as recited by independent claim 1. This is because, in *Wesinger*, "[w]hen a <u>connection request</u> is received, the firewall spawns a process, or execution thread, to create a virtual host VHn to handle that connection request." (*Wesinger* at 15:9-12, emphasis added.) *Wesinger*'s DNS processing, on the other hand, "**operates in the usual manner**" to return an IP address (*Wesinger* 9:17), and is not seen to perform the virtual host process, or a "determin[ation] whether the request to look up the IP address transmitted in step (1) corresponds to a device that accepts an encrypted channel connection with the client device." Accordingly, *Wesinger* is not seen to disclose or suggest the features of claim 1.

Additionally, *Wesinger* is not concerned with "determining whether the request to look up the IP address . . . corresponds to a device that accepts an encrypted channel connection with the client device," as recited by claim 1. *Wesinger* merely discloses that encryption may be used after a connection is established. (*See Wesinger* at 4:39-42; 12:22-28.) For this additional reason, *Wesinger* is not seen to disclose or suggest the claimed "determining" feature.

Claim 1 additionally recites "(3) in response to determining, in step (2), that the request to look up the IP address in step (2) corresponds to a device that accepts an encrypted communications channel connection with the client device, providing provisioning information required to initiate the creation of the encrypted communications channel between the client device and the target device . . . ." *Wesinger* is not seen to disclose or suggest this feature for at least two reasons.

First, since *Wesinger* is not understood to disclose the claimed "determining" step, *Wesinger* also cannot disclose the "providing" step, which is "in response to determining." Second, *Wesinger* states that, "[o]nce a connection has been allowed, the virtual host process invokes code that performs . . . channel processing (encryption . . .)." (*Id.* at 17:1-7.) But a review of *Wesinger* does not reveal that performing encryption involves providing any provisioning information required to initiate the creation of an encrypted channel, much less doing so in response to a determination from a request to look up an IP address. Indeed, *Wesinger* only briefly mentions encryption and is not seen to describe the particulars of how it might be implemented. Accordingly, *Wesinger* is not seen to to disclose or suggest the "providing" feature of claim 1.

To support an obvious rejection, "<u>all of the claim limitations</u> must be taught or suggested by the prior art applied and that <u>all words</u> in a claim must be considered in judging the patentability of that claim against the prior art." *Ex Parte Karl Burgess*, Appeal 2008-2820, 2009 WL 291172 (B.P.A.I. 2009), at *3 (citing *In re Royka*, 490 F.2d 981, 984-85 (CCPA 1974), *In re Wilson*, 424 F.2d 1382, 1385 (CCPA 1970)) (emphasis added). A rejection based on obviousness "cannot be sustained with mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *KSR Int'l Co. v. Teleflex Inc.*, 126 S. Ct. 1727, 1741 (2007) (citing *In re Kahn*, 441 F.3d at 988).

Since *Wesinger* is not seen to teach or suggest all of the claimed elements, a *prima facie* case of obviousness has not been established with respect to claim 1. Amended independent claim 19 is different in scope but contains similar features to those discussed above for claim 1. Accordingly, for reasons similar to those identified above for claim 1, *Wesinger* is not seen to teach or suggest all of the claimed elements of claim 19.

The other claims currently under consideration in the application (claims 2, 4-10, 12, 18, and 20-37) are dependent from their respective independent claims discussed above and therefore are believed to be allowable for at least similar reasons. Additionally, the dependent claims are allowable for the additional reason that one or more features recited therein are not disclosed or suggested by the cited references. Because each dependent claim is deemed to define an additional aspect of the invention, individual consideration of each on its own merits is respectfully requested. Accordingly, reconsideration and withdrawal of the rejection of dependent claims 2, 4-10, 12, 18, and 20 are respectfully requested.

CONCLUSION

Applicants respectfully submit that all of the pending claimsare in condition for allowance. If any questions remain, or should the present response not place the claims in condition for allowance, Applicants respectfully invite the Examiner to contact the undersigned attorney so that any such matters may be promptly resolved.

Any remarks in support of patentability of one claim should not be imputed to any other claim, even if similar terminology is used. Any remarks referring to only a portion of a claim should not be understood to base patentability on that portion; rather, patentability rests on each claim taken as a whole. 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 intent to concede any issue with regard to any claim, 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.

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 501133 and please credit any excess fees to such deposit account.

Respectfully submitted,

MCDERMOTT WILL & EMERY LLP
/Kenneth C. Cheney/

Kenneth C. Cheney
Registration No. 61,841

Please recognize our Customer No. 23630 as our correspondence address

4 Park Plaza, Suite 1700
Irvine, CA 92614-2559
Phone: (949) 851-0633
Facsimile: (949) 851-9348 KCC:kcc
Date: November 1, 2013

Electronic Patent Application Fee Transmittal

Application Number:	13615557
Filing Date:	13-Sep-2012
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Kenneth C. Cheney/Kimila Carraway
Attorney Docket Number:	077580-0177

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:				
Claims in Excess of 20	1202	14	80	1120
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
		Total in USD ($)		**1120**

Electronic Acknowledgement Receipt

EFS ID:	17298435
Application Number:	13615557
International Application Number:	
Confirmation Number:	1089
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Kenneth C. Cheney/Kimila Carraway
Filer Authorized By:	Kenneth C. Cheney
Attorney Docket Number:	077580-0177
Receipt Date:	01-NOV-2013
Filing Date:	13-SEP-2012
Time Stamp:	22:30:00
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1120
RAM confirmation Number	6804
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		077580-0177_Amendment.pdf	137957 29066171a1eae88a787dce80935be61e9871071f	yes	12

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Claims	2	6
Applicant Arguments/Remarks Made in an Amendment	7	12

Warnings:

Information:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
2	Fee Worksheet (SB06)	fee-info.pdf	30373 d0652f160340346731f76a952e21ae0b1507d8f3	no	2

Warnings:

Information:

Total Files Size (in bytes):	168330

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 (09-11)
Approved for use through 1/31/2014. 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.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/615,557	Filing Date 09/13/2012	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	NUMBER FILED (Column 1)	NUMBER EXTRA (Column 2)	RATE ($)	FEE ($)
☒ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	**380**
☒ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	**620**
☒ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	**250**
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	* 0	x $60 =	**0**
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2 minus 3 =	* 0	x $250 =	**0**
☐ 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).			
☐ 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	**1250**

APPLICATION AS AMENDED – PART II

AMENDMENT	**11/01/2013**	CLAIMS REMAINING AFTER AMENDMENT (Column 1)		HIGHEST NUMBER PREVIOUSLY PAID FOR (Column 2)	PRESENT EXTRA (Column 3)	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 34	Minus	** 20	= 14	x $80 =	1120
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	x $420 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	**1120**

AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT (Column 1)		HIGHEST NUMBER PREVIOUSLY PAID FOR (Column 2)	PRESENT EXTRA (Column 3)	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						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.

LIE
/DIANE JOHNSON/

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.
13/615,557	09/13/2012	Victor Larson	077580-0177	1089

23630 7590 11/13/2013
McDermott Will & Emery
The McDermott Building
500 North Capitol Street, N.W.
Washington, DC 20001

EXAMINER	
LIM, KRISNA	
ART UNIT	**PAPER NUMBER**
2453	

NOTIFICATION DATE	DELIVERY MODE
11/13/2013	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. 13/615,557	Applicant(s) LARSON ET AL.	
	Examiner KRISNA LIM	Art Unit 2453	AIA (First Inventor to File) Status No

-- 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 *11/01/2013*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on ______.

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) *1,2,4-10,12 and 14-37* 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) *1,2,4-10,12 and 14-37* is/are rejected.

8)☐ Claim(s) ______ is/are objected to.

9)☐ Claim(s) ______ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

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).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some * c)☐ None of the:

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) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date ______.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. ______ .

4) ☐ Other: ______.

1. The present application is being examined under the pre-AIA first to invent provisions.

2. Claims 1-2, 4-10, 12 and 14-00 are still pending for examination. Claims 21-37 are newly added for examination. Claims 3, 11 and 13 have been canceled.

3. 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 LongL* 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Omum,* 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).

4. Claims 1, 2, 4-10, 12 and 14-37 are rejected on the ground of nonstatutory obviousness-type
double patenting as being unpatentable over claims 1-18 of U.S. Patent No. 7,933,990.

Although the conflicting claims are not identical, they are not patentably distinct from each other because they all directed to a method of transparently creating an encrypted communication channel (i.e. automatically initiating an encrypted communication channel) between a client device and a target device based on a

determination that a request access to a device that accepts an encrypted communication channel. The difference is the current application claimed language of **"supports secure communications audio/video".** It would have been obvious to one of ordinary skill in the art to recognize that such additional claimed language" **supports communications** audio/video" would have been a matter of use and such feature is well known and it would not be a patentably distinguishable feature.

5. Claims 1, 2, 4-10, 12 and 14-37 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-3, 5-9 and 11-15 of U.S. Patent No. 7,490,151.

Although the conflicting claims are not identical, they are not patentably distinct from each other because they are directed to a method of **transparently creating** an encrypted communication channel (i.e. automatically initiating an encrypted communication channel) between a client device and a target device based on a determination that a request access to a device that accepts an encrypted communication channel. The difference is the current application claimed language of **"supports secure communications audio/video".** It would have been obvious to one of ordinary skill in the art to recognize that such additional claimed language" **supports communications** audio/video" would have been a matter of use and such feature is well known and it would not be a patentably distinguishable feature.

6. Claims 1, 2, 4-10, 12 and 14-37 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-9 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 method of transparently creating an encrypted communication channel (i.e. **transparently creating a virtual private network)** between a client device and a target device based on a determination that a request access to a device that accepts an encrypted communication channel. The difference is the current application claimed language of **"supports secure communications audio/video".** It would have been obvious to one of ordinary skill in the art to recognize that such additional claimed language" supports communications audio/video" would have been a matter of use and such feature is well known and it would not be a patentably distinguishable feature.

7. In response to the above rejection, applicants request that the terminal disclaimer be held in abeyance until the claims are indicated to be allowable. Claims 1-2, 4-10, 12 and 14-37 would be allowable when the terminal disclaimers are submitted and approved.

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

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.

Kl
November 06, 2013

/Krisna Lim/
Primary Examiner Art Unit 2453

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13615557	LARSON ET AL.
	Examiner	**Art Unit**
	KRISNA LIM	2453

CPC- SEARCHED

Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED

Symbol	Date	Examiner

US CLASSIFICATION SEARCHED

Class	Subclass	Date	Examiner
709	222-227	07/25/2013	kl

SEARCH NOTES

Search Notes	Date	Examiner
Inventors	07/25/2013	kl

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

Index of Claims

Application/Control No.	Applicant(s)/Patent Under Reexamination
13615557	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	07/25/2013	11/06/2013							
	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		✓							
	29		✓							
	30		✓							
	31		✓							
	32		✓							
	33		✓							
	34		✓							
	35		✓							
	36		✓							

Index of Claims	Application/Control No. 13615557	Applicant(s)/Patent Under Reexamination LARSON ET AL.
	Examiner KRISNA LIM	Art Unit 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	07/25/2013	11/06/2013							
	37		✓							

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	**13/615,557**
Filing Date	**09-13-2012**
First Named Inventor	**Victor Larson**
Art Unit	**2453**
Examiner Name	**Krisna Lim**
Docket Number	**77580-177 (VRNK-0001CP3CON8)**

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
	A170	6,434,600	08/13/2002	Waite et al.	
	A171	7,225,249	05/29/2007	Barry et al.	

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
	B23	US2002/0004826	01/10/2002	Waite et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3-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.	
	D1413	Notice of Allowance dated August 9, 2013 from Corresponding U.S. Application Number 13/474,397	
	D1414	Office Action dated August 19, 2013 from Corresponding U.S. Application Number 13/903,788	

EXAMINER	DATE CONSIDERED
/Krisna Lim/	11/05/2013

*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	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

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 any required fees 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/ Date: September 30, 2013

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 45414536-1.077580.0177

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	**13/615,557**
Filing Date	**09-13-2012**
First Named Inventor	**Victor Larson**
Art Unit	**2453**
Examiner Name	**Krisna Lim**
Docket Number	**77580-177 (VRNK-0001CP3CON8)**

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
	A172	6,011,579	01/04/2000	Newlin	
	A173	8,504,696	08/06/2013	Larson et al.	
	A174	8,504,697	08/06/2013	Larson et al.	
	A175	6,335,966	01/01/2002	Toyoda	
	A176	6,195,677	02/27/2001	Utsumi	
	A177	6,959,184	10/25/2005	Byers et al.	

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 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	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.	
	D1415	Office Action dated October 1, 2013 from Corresponding U.S. Patent Application Number 13/911,813 (077580-0197)	

EXAMINER /Krisna Lim/	DATE CONSIDERED 11/05/2013

*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./

<table>
<tr><td colspan="4" rowspan="6">Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)</td><td colspan="2">Complete if Known</td></tr>
<tr><td>Application Number</td><td>13/615,557</td></tr>
<tr><td>Filing Date</td><td>09-13-2012</td></tr>
<tr><td>First Named Inventor</td><td>Victor Larson</td></tr>
<tr><td>Art Unit</td><td>2453</td></tr>
<tr><td>Examiner Name</td><td>Krisna Lim</td></tr>
<tr><td></td><td></td><td></td><td></td><td>Docket Number</td><td>77580-177 (VRNK-0001CP3CON8)</td></tr>
</table>

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 any required fees 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/

Date: September 30, 2013

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 45488253-1.077580.0177

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	**13/615,557**
Filing Date	**09-13-2012**
First Named Inventor	**Victor Larson**
Art Unit	**2453**
Examiner Name	**Krisna Lim**
Docket Number	**77580-177 (VRNK-0001CP3CON8)**

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
	A178	6,058,250	05/02/2000	Harwood et al.	

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 Code3 -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	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.	
	D1416	Office Action dated October 10, 2013 from Corresponding U.S. Patent Application Number 13/950,877 (077580-0198)	

EXAMINER /Krisna Lim/	DATE CONSIDERED 11/05/2013

*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	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

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 any required fees 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/

Date: October 16, 2013

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 45906357-1.077580.0177

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

RESPONSE UNDER 37 CFR 1.116 - EXPEDITED PROCEDURE
TECHNOLOGY CENTER 2400

Docket No.: 077580-0177
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Victor LARSON, *et al.*	:	Customer Number: 23630
Application No.: 13/615,557	:	Confirmation No. 1089
Filed: September 13, 2012	:	Group Art Unit: 2453
For: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES	:	Examiner: Krisna Lim

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

RESPONSE AFTER FINAL REJECTION
UNDER 37 CFR § 1.116

Commissioner:

In response to the final Office Action dated November 13, 2013, please enter and consider the following:

A **Listing of the Claims** is provided on page 2 of this paper.

Remarks begin on page 8 of this paper.

IN THE CLAIMS

This listing of claims is provided for the sole convenience of the Examiner. No claims have been amended herein.

LISTING OF CLAIMS:

1. (Previously Presented) A method of transparently creating an encrypted communications channel between a client device and a target device, each device being configured to allow secure data communications between the client device and the target device over the encrypted communications channel once the encrypted communications channel is created, the method comprising:

(1) intercepting from the client device a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device;

(2) determining whether the request to look up the IP address transmitted in step (1) corresponds to a device that accepts an encrypted channel connection with the client device; and

(3) in response to determining, in step (2), that the request to look up the IP address in step (2) corresponds to a device that accepts an encrypted communications channel connection with the client device, providing provisioning information required to initiate the creation of the encrypted communications channel between the client device and the target device such that the encrypted communications channel supports secure data communications transmitted between the two devices, the client device being a device at which a user accesses the encrypted communications channel.

2. (Previously Presented) The method of claim 1, wherein providing the provisioning information required to initiate the encrypted communications channel is based on a determination that the target device is a device with which an encrypted communications channel can be established when the IP address request corresponds to a target device identified in an network address lookup.

3. (Canceled)

4. (Previously Presented) The method of claim 1, wherein the domain name is a secure domain name.

5. (Original) The method of claim 1, wherein the encrypted communications channel is a broadband connection.

6. (Original) The method of claim 1, wherein the encrypted communications channel is an unmodulated transmission link.

7. (Previously Presented) The method of claim 1, wherein the encrypted communications channel is a modulated transmission link.

8. (Previously Presented) The method of claim 1, wherein the encrypted communications channel supports at least one of the following: FDM, TDM and CDMA.

9. (Original) The method of claim 1, wherein the client device is a phone.

10. (Previously Presented) The method of claim 9, wherein providing the provisioning information required to initiate the encrypted communications channel is based on a determination that the target device is a device with which an encrypted communications channel can be established when the IP address request corresponds to a target device identified in an network address lookup.

11. (Canceled)

12. (Previously Presented) The method of claim 9, wherein the domain name is a secure domain name.

13. (Canceled)

14. (Original) The method of claim 9, wherein the encrypted communications channel is an unmodulated transmission link.

15. (Original) The method of claim 9, wherein the encrypted communications channel is a modulated transmission link.

16. (Previously Presented) The method of claim 9, wherein the encrypted communications channel supports at least one of the following: FDM, TDM and CDMA.

17. (Previously Presented) The method of claim 1, wherein the target device is a server.

18. (Previously Presented) The method of claim 1, wherein the target device is a phone.

19. (Previously Presented) A system for transparently creating an encrypted communications channel between a client device and a target device, each device being configured to allow secure data communications therebetween over an encrypted communications channel once the encrypted communications channel is created, the system including a memory storing instructions, and a server configuration arranged to:

(1) intercept from the client device a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device;

(2) determine whether the request to look up the IP address transmitted in step (1) corresponds to a device that accepts an encrypted channel connection with the client device; and

(3) in response to determining, in step (2), that the request to look up the IP address corresponds to a device that accepts an encrypted communications channel connection with the client device, provide provisioning information required to initiate the creation of the encrypted communications channel between the client device and the target device such that the encrypted communications channel supports secure data communications transmitted between the two

devices, the client device being a device at which a user accesses the encrypted communications channel.

20. (Previously Presented) A system according to claim 19, wherein the encrypted communications channel supports a plurality of services.

21. (Previously Presented) The system according to claim 19, wherein the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof.

22. (Previously Presented) The system according to claim 21, wherein the plurality of other application programs comprises at least one of the following: e-mail, a word processing program, and telephony.

23. (Previously Presented) The system according to claim 19, wherein the domain name is a secure domain name.

24. (Previously Presented) The system according to claim 19, wherein the encrypted communications channel is a broadband connection.

25. (Previously Presented) The system according to claim 19, wherein the encrypted communications channel is an unmodulated transmission link.

26. (Previously Presented) The system according to claim 19, wherein the encrypted communications channel is a modulated transmission link.

27. (Previously Presented) The system according to claim 19, wherein the encrypted communications channel supports at least one of the following: FDM, TDM and CDMA.

28. (Previously Presented) The system according to claim 19, wherein the client device is a phone.

29. (Previously Presented) The system according to claim 19, wherein the target device is a server.

30. (Previously Presented) The system according to claim 19, wherein the target device is a phone.

31. (Previously Presented) The system according to claim 19, wherein intercepting the request consists of the system receiving the request to determine whether the target device accepts an encrypted channel connection with the client device.

32. (Previously Presented) The system according to claim 19, wherein intercepting the request occurs within another device that is separate from the client device.

33. (Previously Presented) The method according to claim 1, wherein intercepting the request consists of receiving the request to determine whether the target device accepts an encrypted channel connection with the client device.

34. (Previously Presented) The method according to claim 1, wherein the intercepting the request occurs within another device that is separate from the client device.

35. (Previously Presented) The method according to claim 1, wherein the encrypted communications channel supports a plurality of services.

36. (Previously Presented) The method according to claim 35, wherein the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof.

37. (Previously Presented) The method according to claim 36, wherein the plurality of other application programs comprises at least one of the following: e-mail, a word processing program, and telephony.

REMARKS

Claims 1, 2, 4-10, 12, and 14-37 are pending in the application, with claims 1 and 19 being the independent claims. No claims have been amended. However, a listing of the pending claims is provided herewith for the Examiner's convenience. Reconsideration and withdrawal of the rejections are respectfully requested.

Claim Rejection – Double Patenting

Claims 1, 2, 4-10, 12, and 14-37 are rejected on the ground of nonstatutory obviousness-type double patenting over various claims of U.S. Patent Nos. 7,933,990, 7,490,151, and 6,502,135. Without conceding the correctness of the double patenting rejections, to expedite the allowance of this application, Applicants are submitting Terminal Disclaimers for the '990, '151, and '135 patents to obviate the double patenting rejections. Applicants note that the filing of a terminal disclaimer is not an admission of the propriety of the rejection. M.P.E.P. § 804.02 *citing Quad Environmental Technologies Corp. v. Union Sanitary District*, 946 F.2d 870, 20 USPQ2d 1392 (Fed. Cir. 1991).

Since the double patenting rejections are the sole remaining issues in the Office Action the application is believed to be in condition for allowance and such action is respectfully requested.

CONCLUSION

Applicants respectfully submit that all of the pending claims are in condition for allowance. If any questions remain, or should the present response not place the claims in condition for allowance, Applicants respectfully invite the Examiner to contact the undersigned attorney so that any such matters may be promptly resolved.

Any remarks in support of patentability of one claim should not be imputed to any other claim, even if similar terminology is used. Any remarks referring to only a portion of a claim should not be understood to base patentability on that portion; rather, patentability rests on each claim taken as a whole. 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 intent to concede any issue with regard to any claim, 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.

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 501133 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

/Kenneth C. Cheney/

Kenneth C. Cheney
Registration No. 61,841

4 Park Plaza, Suite 1700
Irvine, CA 92614-2559
Phone: (949) 851-0633
Facsimile: (949) 851-9348 KCC:kcc
Date: February 13, 2014

Please recognize our Customer No. 23630 as our correspondence address

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT

Docket Number (Optional)
077580-0177

In re Application of: Victor LARSON, et al.

Application No.: 13/615,557

Filed: September 13, 2012

For: 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. 61,841

/Kenneth C. Cheney/ — Signature
February 13, 2014 — Date

Kenneth C. Cheney
Typed or printed name

(949) 851-0633
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.

Electronic Patent Application Fee Transmittal

Application Number:	13615557
Filing Date:	13-Sep-2012
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Kenneth C. Cheney/Kimila Carraway
Attorney Docket Number:	077580-0177

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($)
Miscellaneous:				
Statutory or Terminal Disclaimer	1814	3	160	480
		Total in USD ($)		**480**

Electronic Acknowledgement Receipt

EFS ID:	18202047
Application Number:	13615557
International Application Number:	
Confirmation Number:	1089
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Kenneth C. Cheney/Kimila Carraway
Filer Authorized By:	Kenneth C. Cheney
Attorney Docket Number:	077580-0177
Receipt Date:	13-FEB-2014
Filing Date:	13-SEP-2012
Time Stamp:	20:36:36
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$480
RAM confirmation Number	4785
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		077580-0177_Response_After_Final_Rejection.pdf	6502891 2b56caad62b7b7584b8a67bd6145b993087c906d	yes	12

Multipart Description/PDF files in .zip description

Document Description	Start	End
Response After Final Action	1	1
Claims	2	7
Applicant Arguments/Remarks Made in an Amendment	8	9
Terminal Disclaimer Filed	10	10
Terminal Disclaimer Filed	11	11
Terminal Disclaimer Filed	12	12

Warnings:

Information:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
2	Fee Worksheet (SB06)	fee-info.pdf	30453 fedda7192c607ceb98ce31501dd6a7ce6c5b36a0	no	2

Warnings:

Information:

Total Files Size (in bytes): 6533344

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.

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT	Docket Number (Optional) 077580-0177

In re Application of: Victor LARSON, et al.

Application No.: 13/615,557

Filed: September 13, 2012

For: 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. 7,490,151 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. 61,841

/Kenneth C. Cheney/ — Signature

February 13, 2014 — Date

Kenneth C. Cheney — Typed or printed name

(949) 851-0633 — 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.

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) 077580-0177

In re Application of: Victor LARSON, et al.

Application No.: 13/615,557

Filed: September 13, 2012

For: 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. 7,933,990 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. 61,841

/Kenneth C. Cheney/ — Signature
February 13, 2014 — Date

Kenneth C. Cheney — Typed or printed name

(949) 851-0633 — 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.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/615,557	Filing Date 09/13/2012	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	NUMBER FILED (Column 1)	NUMBER EXTRA (Column 2)	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	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 $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).			
☐ 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	

APPLICATION AS AMENDED – PART II

AMENDMENT	02/13/2014	CLAIMS REMAINING AFTER AMENDMENT (Column 1)		HIGHEST NUMBER PREVIOUSLY PAID FOR (Column 2)	PRESENT EXTRA (Column 3)	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 34	Minus	** 34	= 0	x $80 =	0
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	x $420 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	**0**

AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT (Column 1)		HIGHEST NUMBER PREVIOUSLY PAID FOR (Column 2)	PRESENT EXTRA (Column 3)	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						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.

LIE
/DEBORAH NASH/

Application Number	Application/Control No.	Applicant(s)/Patent under Reexamination	
	13/615,557	LARSON ET AL.	

Document Code - DISQ	Internal Document – DO NOT MAIL

TERMINAL DISCLAIMER	☐ APPROVED	☒ DISAPPROVED
Date Filed : 2/13/14	**This patent is subject to a Terminal Disclaimer**	

Approved/Disapproved by:

The person who signed the terminal disclaimer:

[ ] has failed to state his/her capacity to sign for the business entity. (See FP 14.28)

[ ] is not recognized as an officer of the assignee. (See FP 14.29)

[x] does not have power of attorney. (FP 14.29.01)

No fee is requried.

Jean Proctor

U.S. 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.
13/615,557	09/13/2012	Victor Larson	077580-0177	1089

23630 7590 02/25/2014
McDermott Will & Emery
The McDermott Building
500 North Capitol Street, N.W.
Washington, DC 20001

EXAMINER	
LIM, KRISNA	
ART UNIT	**PAPER NUMBER**
2453	

NOTIFICATION DATE	DELIVERY MODE
02/25/2014	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. 13/615,557	Applicant(s) LARSON ET AL.	
	Examiner KRISNA LIM	Art Unit 2453	AIA (First Inventor to File) Status No

-- 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 MONTHS 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 *02/13/2014*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

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) *1,2,4-10,12 and 14-37* 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, 2, 4-10, 12 and 14-37* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

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).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

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) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

1. The present application is being examined under the pre-AIA first to invent provisions.

2. Claims 1-2, 4-10, 12 and 14-00 are still pending for examination. Claims 21-37 are newly added for examination. Claims 3, 11 and 13 have been canceled.

3. 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 LongL* 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Omum,* 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).

4. Claims 1, 2, 4-10, 12 and 14-37 are rejected on the ground of nonstatutory obviousness-type
double patenting as being unpatentable over claims 1-18 of U.S. Patent No. 7,933,990.

Although the conflicting claims are not identical, they are not patentably distinct from each other because they all directed to a method of transparently creating an encrypted communication channel (i.e. automatically initiating an encrypted communication channel) between a client device and a target device based on a

determination that a request access to a device that accepts an encrypted communication channel. The difference is the current application claimed language of **"supports secure communications audio/video".** It would have been obvious to one of ordinary skill in the art to recognize that such additional claimed language" **supports communications** audio/video" would have been a matter of use and such feature is well known and it would not be a patentably distinguishable feature.

5. Claims 1, 2, 4-10, 12 and 14-37 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-3, 5-9 and 11-15 of U.S. Patent No. 7,490,151.

Although the conflicting claims are not identical, they are not patentably distinct from each other because they are directed to a method of **transparently creating** an encrypted communication channel (i.e. automatically initiating an encrypted communication channel) between a client device and a target device based on a determination that a request access to a device that accepts an encrypted communication channel. The difference is the current application claimed language of **"supports secure communications audio/video".** It would have been obvious to one of ordinary skill in the art to recognize that such additional claimed language" **supports communications** audio/video" would have been a matter of use and such feature is well known and it would not be a patentably distinguishable feature.

6. Claims 1, 2, 4-10, 12 and 14-37 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-9 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 method of transparently creating an encrypted communication channel (i.e. **transparently creating a virtual private network)** between a client device and a target device based on a determination that a request access to a device that accepts an encrypted communication channel. The difference is the current application claimed language of **"supports secure communications audio/video".** It would have been obvious to one of ordinary skill in the art to recognize that such additional claimed language" supports communications audio/video" would have been a matter of use and such feature is well known and it would not be a patentably distinguishable feature.

7. On February 13, 2014, in response to the above rejection, applicants submitted 3 terminal disclaimers but they have not been approved. Claims 1-2, 4-10, 12 and 14-37 would be allowable when the terminal disclaimers are submitted and approved.

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

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.

Kl
February 19, 2014

/Krisna Lim/
Primary Examiner Art Unit 2453

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13615557	LARSON ET AL.
	Examiner	**Art Unit**
	KRISNA LIM	2453

CPC- SEARCHED

Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED

Symbol	Date	Examiner

US CLASSIFICATION SEARCHED

Class	Subclass	Date	Examiner
709	222-227	07/25/2013	kl

SEARCH NOTES

Search Notes	Date	Examiner
Inventors	07/25/2013	kl

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

Index of Claims	Application/Control No. 13615557	Applicant(s)/Patent Under Reexamination LARSON ET AL.
	Examiner KRISNA LIM	Art Unit 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	07/25/2013	11/06/2013	02/19/2014						
	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		✓	✓						
	29		✓	✓						
	30		✓	✓						
	31		✓	✓						
	32		✓	✓						
	33		✓	✓						
	34		✓	✓						
	35		✓	✓						
	36		✓	✓						

Index of Claims	Application/Control No. 13615557	Applicant(s)/Patent Under Reexamination LARSON ET AL.
	Examiner KRISNA LIM	Art Unit 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	07/25/2013	11/06/2013	02/19/2014						
	37		✓	✓						

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 Number: 23630

OR

☐ Practitioner(s) named below (if more than ten patent 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 Number:

OR

☐ Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone			Email		

Assignee Name and Address:

VirnetX, Inc.
308 Dorla Court , Suite 206
Zephyr Cove, Nevada 89448

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	[signature]	Date	1/30/2013
Name	Sameer Mathur	Telephone	775-548-1785
Title	Vice President - Corporate Development and Marketing		

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: Victor LARSON, et al.

Application No./Patent No.: 13/615,557 Filed/Issue Date: September 13, 2012

Titled: 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. [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: Victor Larson, et al. To: Science Applications International Corporatio
The document was recorded in the United States Patent and Trademark Office at
Reel 027613, Frame 0163, or for which a copy thereof is attached.

2. From: Science Applications International Corporatio To: VirnetX, Inc.
The document was recorded in the United States Patent and Trademark Office at
Reel 027613, Frame 0168, 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.

/Toby H. Kusmer/ April 8, 2014
Signature Date

Toby H. Kusmer, Registration No. 26,418 Attorney for Assignee
Printed or Typed Name Title

Electronic Acknowledgement Receipt

EFS ID:	18710002
Application Number:	13615557
International Application Number:	
Confirmation Number:	1089
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kimila Carraway
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	077580-0177
Receipt Date:	08-APR-2014
Filing Date:	13-SEP-2012
Time Stamp:	21:18:37
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		077580-0177_POA.pdf	581324 ecfda7acbf055a8dbf449b55c66d94e478486d0f	yes	2

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Power of Attorney	1	1
	Assignee showing of ownership per 37 CFR 3.73.	2	2

Warnings:

Information:

Total Files Size (in bytes):	581324

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
13/615,557	09/13/2012	Victor Larson	077580-0177

CONFIRMATION NO. 1089

POA ACCEPTANCE LETTER

OC000000067744328

23630
McDermott Will & Emery
The McDermott Building
500 North Capitol Street, N.W.
Washington, DC 20001

Date Mailed: 04/15/2014

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 04/08/2014.

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.

/zabraha/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

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
13/615,557	09/13/2012	Victor Larson	077580-0177

CONFIRMATION NO. 1089

POWER OF ATTORNEY NOTICE

OC000000067744305

23630
McDermott Will & Emery
The McDermott Building
500 North Capitol Street, N.W.
Washington, DC 20001

Date Mailed: 04/15/2014

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 04/08/2014.

- 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).

/zabraha/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PTO/SB/30EFS (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	13/615,557	Filing Date	2012-09-13	Docket Number (if applicable)	077580-0177	Art Unit	2453
First Named Inventor	Victor LARSON			Examiner Name	Krisna Lim		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

- ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on ______
- ☐ Other ______

☒ Enclosed

- ☒ Amendment/Reply
- ☐ Information Disclosure Statement (IDS)
- ☐ Affidavit(s)/ Declaration(s)
- ☒ Other
  An Information Disclosure Statement is being submitted by mail concurrently with this filing.

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months ______
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other ______

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 501133

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature
☐ Applicant Signature

Signature of Registered U.S. Patent Practitioner			
Signature	/Toby H. Kusmer/	Date (YYYY-MM-DD)	2014-05-27
Name	Toby H. Kusmer	Registration Number	26418

Docket No.: 077580-0177
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Victor LARSON, *et al.*	:	Customer Number: 23630
Application No.: 13/615,557	:	Confirmation No. 1089
Filed: September 13, 2012	:	Group Art Unit: 2453
For: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES	:	Examiner: Krisna Lim

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

RESPONSE SUBMITTED WITH REQUEST FOR CONTINUED EXAMINATION

Commissioner:

In response to the final Office Action dated February 25, 2014, please enter and consider the following:

Remarks begin on page 2 of this paper.

DM_US 52503637-1.077580.0177

REMARKS

Claims 1, 2, 4-10, 12, and 14-37 are pending in the application, with claims 1 and 19 being the independent claims. No claims have been amended. Reconsideration and withdrawal of the rejections are respectfully requested.

Claim Rejection – Double Patenting

Claims 1, 2, 4-10, 12, and 14-37 are rejected on the ground of nonstatutory obviousness-type double patenting over various claims of U.S. Patent Nos. 7,933,990, 7,490,151, and 6,502,135. Applicants filed a Response on February 13, 2014, together with three Terminal Disclaimers. The Terminal Disclaimers were rejected because a proper Power of Attorney was not on file for the application. A Power of Attorney was submitted on April 8, 2014, and was accepted by the Office on April 15, 2014.

Applicants are re-submitting Terminal Disclaimers for the '990, '151, and '135 patents to obviate the double patenting rejections. Applicants note that the filing of a terminal disclaimer is not an admission of the propriety of the rejection. M.P.E.P. § 804.02 *citing Quad Environmental Technologies Corp. v. Union Sanitary District*, 946 F.2d 870, 20 USPQ2d 1392 (Fed. Cir. 1991).

Since the double patenting rejections are the sole remaining issues in the Office Action the application is believed to be in condition for allowance and such action is respectfully requested.

CONCLUSION

Applicants respectfully submit that all of the pending claims are in condition for allowance. If any questions remain, or should the present response not place the claims in condition for allowance, Applicants respectfully invite the Examiner to contact the undersigned attorney so that any such matters may be promptly resolved.

Any remarks in support of patentability of one claim should not be imputed to any other claim, even if similar terminology is used. Any remarks referring to only a portion of a claim should not be understood to base patentability on that portion; rather, patentability rests on each claim taken as a whole. 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 intent to concede any issue with regard to any claim, 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.

Please charge any fees associated with filing the Terminal Disclaimers under 37 C.F.R. 1.20(d) to Deposit Account 50-1133.

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 50-1133 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Date: May 27, 2014

/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

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

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT	Docket Number (Optional) 077580-0177

In re Application of: Victor LARSON, et al.

Application No.: 13/615,557

Filed: September 13, 2012

For: 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. 26,418

/Toby H. Kusmer/ — May 27, 2014
Signature — Date

Toby H. Kusmer
Typed or printed name

(617) 535-4000
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.

Electronic Patent Application Fee Transmittal

Application Number:	13615557
Filing Date:	13-Sep-2012
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Toby H. Kusmer./Kimila Carraway
Attorney Docket Number:	077580-0177

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($)
Miscellaneous:				
Request for Continued Examination	1801	1	1200	1200
		Total in USD ($)		**1200**

Electronic Acknowledgement Receipt

EFS ID:	19138109
Application Number:	13615557
International Application Number:	
Confirmation Number:	1089
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kimila Carraway
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	077580-0177
Receipt Date:	27-MAY-2014
Filing Date:	13-SEP-2012
Time Stamp:	19:55:07
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1200
RAM confirmation Number	7446
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		077580-0177_RCE_Response.pdf	2540288 85418091d91fbb454ecf1e1489600df90fe647e5	yes	8

Multipart Description/PDF files in .zip description

Document Description	Start	End
Request for Continued Examination (RCE)	1	2
Amendment Submitted/Entered with Filing of CPA/RCE	3	3
Applicant Arguments/Remarks Made in an Amendment	4	5
Terminal Disclaimer Filed	6	6
Terminal Disclaimer Filed	7	7
Terminal Disclaimer Filed	8	8

Warnings:

Information:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
2	Fee Worksheet (SB06)	fee-info.pdf	30566 fd902e5ed8c64984b23e8cbcd104a958be7d8146	no	2

Warnings:

Information:

Total Files Size (in bytes):	2570854

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.

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT

Docket Number (Optional)
077580-0177

In re Application of: Victor LARSON, et al.

Application No.: 13/615,557

Filed: September 13, 2012

For: 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. 7,933,990 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. 26,418

/Toby H. Kusmer/ — Signature

May 27, 2014 — Date

Toby H. Kusmer — Typed or printed name

(617) 535-4000 — 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.

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT	Docket Number (Optional) 077580-0177

In re Application of: Victor LARSON, et al.

Application No.: 13/615,557

Filed: September 13, 2012

For: 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. 7,490,151 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. 26,418

/Toby H. Kusmer/
Signature

May 27, 2014
Date

Toby H. Kusmer
Typed or printed name

(617) 535-4000
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.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/615,557	Filing Date 09/13/2012	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	NUMBER FILED (Column 1)	NUMBER EXTRA (Column 2)	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	34 minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2 minus 3 =	*	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 $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).			
☐ 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	

APPLICATION AS AMENDED – PART II

AMENDMENT	05/27/2014	CLAIMS REMAINING AFTER AMENDMENT (Column 1)		HIGHEST NUMBER PREVIOUSLY PAID FOR (Column 2)	PRESENT EXTRA (Column 3)	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 34	Minus	** 34	=	X $ =	
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	=	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT (Column 1)		HIGHEST NUMBER PREVIOUSLY PAID FOR (Column 2)	PRESENT EXTRA (Column 3)	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						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.

LIE
/PEGGY YARBOROUGH/

05-28-14

IDJ

OPAP MAY 27 2014 PATENT & TRADEMARK OFFICE

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.

TRANSMITTAL FORM (to be used for all correspondence after initial filing)	Application Number	13/615,557
	Filing Date	09-13-2012
	First Named Inventor	Victor Larson
	Art Unit	2453
	Examiner Name	Krisna Lim
Total Number of Pages in This Submission	Attorney Docket Number	77580-177

ENCLOSURES *(Check all that apply)*

- [ ] Fee Transmittal Form
  - [ ] 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

12 Boxes of Non Patent Literature; 11 Foreign Publication References. The Request for Continued Examination is being electronically filed on May 27, 2014 and all fees due will be paid at the time of the RCE filing.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	McDermott, Will @ Emery		
Signature	/Toby H. Kusmer/		
Printed name	Toby H. Kusmer		
Date	May 27, 2014	Reg. No.	26,418

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	

ARTIFACT SHEET

Enter artifact number below. Artifact number is application number + artifact type code (see list below) + sequential letter (A, B, C …). The first artifact folder for an artifact type receives the letter A, the second B, etc.. Examples: 59123456PA, 59123456PB, 59123456ZA, 59123456ZB

13615557ZA

Indicate quantity of a single type of artifact received but not scanned. Create individual artifact folder/box and artifact number for each Artifact Type.

☐ CD(s) containing:
- ☐ computer program listing
  Doc Code: Computer — Artifact Type Code: P
- ☐ pages of specification and/or sequence listing and/or table
  Doc Code: Artifact — Artifact Type Code: S
- ☐ content unspecified or combined
  Doc Code: Artifact — Artifact Type Code: U

☐ Stapled Set(s) Color Documents or B/W Photographs
Doc Code: Artifact — Artifact Type Code: C

☐ Microfilm(s)
Doc Code: Artifact — Artifact Type Code: F

☐ Video tape(s)
Doc Code: Artifact — Artifact Type Code: V

☐ Model(s)
Doc Code: Artifact — Artifact Type Code: M

☐ Bound Document(s)
Doc Code: Artifact — Artifact Type Code: B

☐ Confidential Information Disclosure Statement or Other Documents marked Proprietary, Trade Secrets, Subject to Protective Order, Material Submitted under MPEP 724.02, etc.
Doc Code: Artifact — Artifact Type Code X

[1] Other, description: **BROCHURE**
Doc Code: Artifact — Artifact Type Code: Z

March 8, 2004

Subst. for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*				Application Number	**13/615,557**
				Filing Date	**09-13-2012**
				First Named Inventor	**Victor Larson**
				Art Unit	**2453**
				Examiner Name	**Krisna Lim**
				Docket Number	**77580-177 (VRNK-0001CP3CON8)**

OIPE MAY 27 2014 PATENT & TRADEMARK OFFICE

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; 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.

[ ] The Commissioner is authorized to charge any required fees to Deposit Account 50-1133.

[X] Information Disclosure Statement is being filed with the Request for Continued Examination, which was electronically filed on May 27, 2014 and at that time, all fees due, were paid. However, the Commissioner is hereby authorized to charge any 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/

Date: May 27, 2014

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 52498342-1.077580.0177

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT VS. APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	13/615,557
Filing Date	09-13-2012
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Docket Number	77580-177 (VRNK-0001CP3CON8)

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
	A179	RE39,360	10/17/2006	Aziz et al.	
	A180	5,416,842	05/16/1995	Aziz	
	A181	5,420,926	05/30/1995	Low et al.	
	A182	5,444,782	08/22/1995	Adams, Jr. et al.	
	A183	5,455,861	10/03/1995	Faucher et al.	
	A184	5,530,758	06/25/1996	Marino, Jr. et al.	
	A185	5,623,601	04/22/1997	Vu	
	A186	5,636,139	06/03/1997	McLaughlin et al.	
	A187	5,689,566	11/18/1997	Nguyen	
	A188	5,781,550	07/14/1998	Templin et al.	
	A189	5,805,820	09/08/1998	Bellovin et al.	
	A190	5,812,670	09/22/1998	Micali	
	A191	5,884,270	03/16/1999	Walker et al.	
	A192	5,889,863	03/30/1999	Weber	
	A193	5,915,087	06/22/1999	Hammond et al.	
	A194	5,940,393	08/17/1999	Duree et al.	
	A195	5,961,593	10/05/1999	Gabber et al.	
	A196	5,974,454	10/26/1999	Apfel et al.	
	A197	6,003,084	12/14/1999	Green et al.	
	A198	6,012,088	06/04/2000	Li et al.	
	A199	6,016,504	01/18/2000	Arnold et al.	
	A200	6,023,510	02/08/2000	Epstein	
	A201	6,032,118	02/29/2000	Tello et al.	
	A202	6,055,236	04/25/200	Nessett et al.	
	A203	6,055,518	04/25/2000	Franklin et al.	
	A204	6,055,575	04/25/2000	Paulsen et al.	
	A205	6,073,175	06/06/2000	Tavs et al.	
	A206	6,111,883	08/29/2000	Terada et al.	
	A207	6,148,342	11/14/2000	Ho	
	A208	6,151,628	11/21/2000	Xu et al.	
	A209	6,154,839	11/28/2000	Arrow et al.	
	A210	6,182,072	01/30/2001	Leak et al.	
	A211	6,182,141	01/30/2001	Blum et al.	
	A212	6,199,122	03/06/2001	Wilson	
	A213	6,225,993	05/01/2001	Lindblad et al.	
	A214	6,298,383	10/02/2001	Gutman et al.	
	A215	6,345,361	02/05/2002	Jerger et al.	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	A216	6,366,912	04/02/2002	Wallent et al.	
	A217	6,421,732	07/16/2002	Alkhatib et al.	
	A218	6,426,955	07/30/2002	Gossett et al.	
	A219	6,438,127	08/20/2002	Le Goff et al.	
	A220	6,449,272	09/10/2002	Chuah et al.	
	A221	6,453,034	09/17/2002	Donovan et al.	
	A222	6,490,290	12/03/2002	Zhang et al.	
	A223	6,496,491	12/17/2002	Chuah et al.	
	A224	6,564,261	05/13/2003	Gudjonsson et al.	
	A225	6,590,588	07/08/2003	Lincke et al.	
	A226	6,591,306	07/08/2003	Redlich	
	A227	6,606,660	08/12/2003	Bowman-Amuah	
	A228	6,609,196	08/19/2003	Dickinson III et al.	
	A229	6,636,505	10/21/2003	Wang et al.	
	A230	6,640,302	10/28/2003	Subramaniam et al.	
	A231	6,643,701	11/04/2003	Aziz et al.	
	A232	6,687,823	02/03/2004	Al-Salqan et al.	
	A233	6,693,878	02/17/2004	Daruwalla et al.	
	A234	6,751,729	06/15/2004	Giniger et al.	
	A235	6,754,212	06/22/2004	Terada et al.	
	A236	6,801,509	10/05/2004	Chuah et al.	
	A237	6,804,783	10/12/2004	Wesinger, Jr. et al.	
	A238	6,829,242	12/07/2004	Davison et al.	
	A239	6,834,271	12/21/2004	Hodgson et al.	
	A240	6,917,600	07/12/2005	Chuah et al.	
	A241	7,028,182	04/11/2006	Killcommons	
	A242	7,065,784	06/20/2006	Hopman et al.	
	A243	7,100,195	08/29/2006	Underwood	
	A244	7,103,770	09/05/2006	Conrath	
	A245	7,203,190	04/10/2007	Ruban et al.	
	A246	7,249,377	07/24/2007	Lita et al.	
	A247	7,307,990	12/11/2007	Rosen et al.	
	A248	6,701,437	03/03/2004	Hoke et al.	
	A249	4,405,829	09/20/1983	Rivest	
	A250	6,502,135	12/31/2002	Munger	
	A251	6,449,657	09/10/2002	Stanbach	
	A252	6,546,003	04/08/2003	Farris	
	A253	6,430,176	08/06/02	Christie	
	A254	6,930,998	08/16/2005	Sylvain	
	A255	6,065,049	05/16/2000	Beser et al.	
	A256	5,412,730	05/02/1995	Jones	

	A257	7,669,049	02/23/2010	Wang et al.	
	A258	4,912,762	03/27/1990	Lee et al.	
	A258	7,275,113	09/25/2007	Araujo	
	A259	6,367,009	04/2002	Davis et al.	

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
	B25	US2002/0006132	01/17/2002	Chuah et al.,	
	B26	US2003/0005132	01/2003	Nguyen et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3 -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
	C29	JP 10-126440	05-15-1998	Hitachi Ltd.		English Abstract	
	C30	JP 11-355272	12-24-1999	Lucent Technol Inc.		English Abstract	
	C31	JP 11-355271	12-24-1999	Lucent Technol Inc.		English Abstract	
	C32	JP 11-261704	09-24-1999	Fujitsu Ltd.		English Abstract	
	C33	JP 10-70576	03-10-1998	Kokusai Denshin Denwa Co. Ltd.		English Abstract	
	C34	GB 2316841	03-04-1998	Kubota Ayumu et al.		English Abstract	
	C35	JP 09-266475	10-07-1997	Hitachi Ltd.		English Abstract	
	C36	JP 10-32610	02-03-1998	NEC Corp.		English Abstract	
	C37	WO 0014938	03-2000	Baehr et al.			
	C38	JP 09-275404	10/21/1997	Nippon Telegr & Teleph Corp.		English Abstract	
	C39	JP 11-167536	06/22/1999	Sun Microsyst Inc.		English Abstract	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

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.	
	D1416	Request for Inter Partes Reexamination of Patent Number 7,490,151 filed on July 25, 2011, Requester Apple Inc. – Exhibit E3: Declaration of James Chester, 13 pages (2011)	
	D1417	Request for Inter Partes Reexamination of Patent Number 7,490,151 filed on July 25, 2011, Requester Apple Inc. – Exhibit A: Curriculum Vitae of James Chester, 4 pages	
	D1418	Request for Inter Partes Reexamination of Patent Number 7,490,151 filed on July 25, 2011, Requester Apple Inc. – Exhibit E1: Declaration of Chris Hopen, 5 pages	
	D1419	Request for Inter Partes Reexamination of Patent Number 7,490,151 filed on July 25, 2011, Requester Apple Inc. – Exhibit E2: Declaration of Michael Fratto, 51 pages (2011)	
	D1420	Request for Inter Partes Reexamination of Patent Number 7,490,151 filed on July 25, 2011, Requester Apple Inc. – Exhibit E: to Michael Fratto's Declaration, Fratto, "Aventail VPN 2.5: Not Your Father's Socks," Network Computing, Vol. 8, No. 18 (October 1, 1997), 3 pages	
	D1421	Request for Inter Partes Reexamination of Patent Number 7,490,151 filed on July 25, 2011, Requester Apple Inc. – Exhibit F: to Michael Fratto's Declaration, Fratto, "Footloose and Fancy Free with Three Socks 5-Based Proxy Servers," Network Computing, Vol. 9, Issue 11, 5 pages (June 15, 1998)	
	D1422	Request for Inter Partes Reexamination of Patent Number 7,490,151 filed on July 25, 2011, Requester Apple Inc. – Exhibit H: to Michael Fratto's Declaration, PR Newswire, "Aventail Ships Directory-enabled Extranet Solution; Aventail Extranet Center v3.1 Available at www.aventail.com." (August 9, 1998), 4 pages	
	D1423	Request for Inter Partes Reexamination of Patent Number 7,490,151 filed on July 25, 2011, Requester Apple Inc. – Exhibit I: to Michael Fratto's Declaration, "Intranet Applications: Briefs," Network World, at page 55 (October 19, 1998), 2 pages	
	D1424	Request for Inter Partes Reexamination of Patent Number 6,502,135 filed on July 11, 2011, Requester Apple Inc. – Exhibit E1: Declaration of Chris Hopen, 5 pages (2011)	
	D1425	Request for Inter Partes Reexamination of Patent Number 6,502,135 filed on July 11, 2011, Requester Apple Inc. – Exhibit E2: Declaration of Michael Fratto, 50 pages	
	D1426	Request for Inter Partes Reexamination of Patent Number 6,502,135 filed on July 11, 2011, Requester Apple Inc. – Exhibit E3: Declaration of James Chester, 13 pages	
	D1427	Request for Inter Partes Reexamination of Patent Number 7,921,211 filed on February 16, 2011, Requester Cisco Systems., - Original Petition to Request Inter Partes Reexamination, 40 pages	
	D1428	Request for Inter Partes Reexamination of Patent Number 8,051,181 filed on March 28, 2012, Requester Apple Inc. – Exhibit C2: Claim Chart – '181 Relative to Mattaway, 9 pages	
	D1429	Request for Inter Partes Reexamination of Patent Number 8,051,181 filed on March 28, 2012, Requester Apple Inc. – Exhibit C6: Claim Chart - '181 Relative to Johnson, 10 pages	
	D1430	Request for Inter Partes Reexamination of Patent Number 8,051,181 filed on March 28, 2012, Requester Apple Inc. – Exhibit C1: Claim Chart '181 Relative to Beser, 9 pages	
	D1431	Request for Inter Partes Reexamination of Patent Number 8,051,181 filed on March 28, 2012, Requester Apple Inc. – Exhibit C3: Claim Chart - '181 Relative to Lendenmann, 9 pages	
	D1432	Request for Inter Partes Reexamination of Patent Number 8,051,181 filed on March 28, 2012, Requester Apple Inc. – Exhibit C4: Claim Chart - '181 Relative to Provino, 9 pages	
	D1433	Request for Inter Partes Reexamination of Patent Number 8,051,181 filed on March 28, 2012, Requester Apple Inc. – Exhibit C5: Claim Chart – '181 Relative to H.323, 9 pages	
	D1434	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Petition for Inter Partes Review, 67 pages	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1435	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1003: Declaration of Michael Fratto Regarding U.S. Patent Number 6,502,135, 195 pages (2013)	
	D1436	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1004: Fratto CV, 3 pages	
	D1437	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1005: Declaration of Chris Hopen Regarding Prior Art and U.S. Patent Number 6,502,135, 25 pages (2013)	
	D1438	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1006: Declaration of James Chester, 26 pages (2013)	
	D1439	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1019: Tittel, E., et al., Windows NT Server 4 for Dummies, Ch. 12, pp. 191-210 (1999)	
	D1440	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1020: Microsoft Windows 98 ResourceKit, 114 pages (1998)	
	D1441	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1024: Ole, "The Internet Protocol Journal, 1(2):1-48 (1998)	
	D1442	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1029: Rescorla, E., et al., RFC 2660, "The Secure HyperText Transfer Protocol," 45 pages (August 1999)	
	D1443	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1030: Lloyd, PPP Authentication Protocols, 15 pages (1992)	
	D1444	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1032: Dierks, "The TLS Protocol Version 1.0," 75 pages (1999)	
	D1445	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1040: Adams, C., et al., RFC 2510, "Internet X.509 Public Key Infrastructure Certificate Management Protocols," 68 pages (March 1999)	
	D1446	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1042: Record of Publication Ex:1015 on IEEE, 2 pages (1996)	
	D1447	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1043: Record of Publication of Reed (Ex. 1015) on ACM Digital Library, 2 pages (1996)	
	D1448	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1044: Record of Publication Ex:1015 on 12th ACSAC, 4 pages (1996)	
	D1449	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1045: Memorandum Opinion dated 7/30/09, 35 pages	
	D1450	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1047: Defendant's Responsive Claim Construction Brief, 37 pages (2011)	
	D1451	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1049: Memorandum Opinion and Order dated April 25, 2012, 31 pages	
	D1452	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1051: Nieh Declaration, 8 pages (2010)	
	D1453	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1057: CV Chris Hopen, 1 page	
	D1454	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1061: Network World Article, 1 page (1998)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1455	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1063: Malkin, G., RFC 2453, "RIP Version 2," 37 pages (November 1998)	
	D1456	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1064:, J Moy, OSPF Version 2, 244 pages, (1998)	
	D1457	IPR2013-00349; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Petition for Inter Partes Review, 73 pages	
	D1458	IPR2013-00349 Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1003: Declaration of Michael Fratto Regarding U.S. Patent Number 6,502,135, 256 pages (2013)	
	D1459	IPR2013-00349 Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1005: Declaration of Chris Hopen Regarding Prior Art and U.S. Patent Number 6,502,135, 25 pages (2013)	
	D1460	IPR2013-00349 Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1006: Declaration of James Chester, 26 pages (2013)	
	D1461	IPR2013-00354; Inter Partes Review of Patent Number 7,490,151 filed on June 17, 2013, Petitioner Apple Inc., – Petition for Inter Partes Review, 73 pages	
	D1462	IPR2013-00354; Inter Partes Review of Patent Number 7,490,151 filed on June 14, 2013, Petitioner Apple Inc., – Exhibit 1003: Declaration of Michael Fratto Regarding U.S. Patent No. 7,490,151, 322 pages (2013)	
	D1463	IPR2013-00354; Inter Partes Review of Patent Number 7,490,151 filed on June 14, 2013, Petitioner Apple Inc., – Exhibit 1005: Declaration of Chris Hopen Regarding Prior Art and U.S. Patent No.: 7,490,151, 23 pages (2013)	
	D1464	IPR2013-00354; Inter Partes Review of Patent Number 7,490,151 filed on June 14, 2013, Petitioner Apple Inc., – Exhibit 1006: Declaration of James Chester, 26 pages (2013)	
	D1465	IPR2013-00354; Inter Partes Review of Patent Number 7,490,151 filed on June 14, 2013, Petitioner Apple Inc., – Exhibit 1048: VirnetX, Inc., Inc. vs. Cisco Systems, Inc., et al., VirnetX Reply Claim Construction Brief of December 19, 2011, 13 pages	
	D1466	IPR2013-00375; Inter Partes Review of Patent Number 6,502,135 filed on June 23, 2013, Petitioner New Bay Capital, LLC., – Petition for Inter Partes Review of Patent No. 6,502,135	
	D1467	IPR2013-00375; Inter Partes Review of Patent Number 6,502,135 filed on June 23, 2013, Petitioner New Bay Capital, LLC., – Exhibit 1002: The 1996 Symposium on Network and Distributed Systems Security (SNDSS'96), Hypermedia Proceedings, Slides, and Summary Report, 57 pages (1996)	
	D1468	IPR2013-00375; Inter Partes Review of Patent Number 6,502,135 filed on June 23, 2013, Petitioner New Bay Capital, LLC., – Exhibit 1005: Windows Sockets, An Open Interface for Network Programming under Microsoft Windows, Version 1.1, 124 pages (1993)	
	D1469	IPR2013-00375; Inter Partes Review of Patent Number 6,502,135 filed on June 23, 2013, Petitioner New Bay Capital, LLC., – Exhibit 1006: eCos Reference Manual, Chapter 38. TCP/IP Library Reference, downloaded from Http://www.ecos.sourceware.org/docs, 3 pages (March 13, 1997)	
	D1470	IPR2013-00375; Inter Partes Review of Patent Number 6,502,135 filed on June 23, 2013, Petitioner New Bay Capital, LLC., – Exhibit 1009: Declaration of Russell Housley Regarding U.S. Patent Number 6,502,135, 105 pages (June 22, 2003)	
	D1471	IPR2013-00375; Inter Partes Review of Patent Number 6,502,135 filed on June 23, 2013, Petitioner New Bay Capital, LLC., – Exhibit 1012: VirnetX Inc., vs. Apple; Transcript of Pretrial Conference on October 18, 2012, 216 pages	
	D1472	IPR2013-00375; Inter Partes Review of Patent Number 6,502,135 filed on June 23, 2013, Petitioner New Bay Capital, LLC., – Exhibit 1013: VirnetX, Inc., vs. Apple: Trial Transcript (Morning Session) of October 31, 2012, 128 pages	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1473	IPR2013-00375; Inter Partes Review of Patent Number 6,502,135 filed on June 23, 2013, Petitioner New Bay Capital, LLC., – Exhibit 1014: Trial Transcript (Morning Session) of November 1, 2012, 146 pages	
	D1474	IPR2013-00375; Inter Partes Review of Patent Number 6,502,135 filed on June 23, 2013, Petitioner New Bay Capital, LLC., – Exhibit 1015: VirnetX Inc., vs. Apple; Memorandum Opinion and Order dated February 26, 2013, 47 pages	
	D1475	IPR2013-00375; Inter Partes Review of Patent Number 6,502,135 filed on June 23, 2013, Petitioner New Bay Capital, LLC., – Exhibit 1018: Virnetx Reply Claim Construction, 13 pages (2011)	
	D1476	IPR2013-00376; Inter Partes Review of Patent Number 7,490,151 filed on June 23, 2013, Petitioner New Bay Capital, LLC. – Petition for Inter Partes Review of U.S. Patent Number 7,490,151, 68 pages	
	D1477	IPR2013-00378; Inter Partes Review of Patent Number 7,921,211 filed on June 23, 2013, Petitioner New Bay Capital, LLC., – Petition for Inter Partes Review of U.S Patent No. 7,921,211	
	D1478	IPR2013-00378; Inter Partes Review of Patent Number 7,921,211 filed on June 23, 2013, Petitioner New Bay Capital, LLC., – Exhibit 1004: Declaration of Russell Housley Regarding U.S. Patent Number 7,418,504, 98 pages (2013)	
	D1479	IPR2013-00378; Inter Partes Review of Patent Number 7,921,211 filed on June 23, 2013, Petitioner New Bay Capital, LLC., – Exhibit 1009: VirnetX, Inc., vs. Mitel Networks Corp., et al., VirnetX Opening Claim Construction Brief, 28 pages (2012)	
	D1480	IPR2013-00378; Inter Partes Review of Patent Number 7,921,211 filed on June 23, 2013, Petitioner New Bay Capital, LLC., – Exhibit 1010: The American Heritage Dictionary of the English Language, Third Edition, 4 pages (1996)	
	D1481	IPR2013-00393; Inter Partes Review of Patent Number 7,418,504 filed on July 1, 2013, Petitioner Apple Inc., – Petition for Inter Partes Review of US Patent No 7,418,504, 62 pages	
	D1482	IPR2013-00393; Inter Partes Review of Patent Number 7,418,504 filed on July 1, 2013, Petitioner Apple Inc., – Exhibit 1003: Declaration of Michael Fratto, 182 pages (2013)	
	D1483	IPR2013-00393; Inter Partes Review of Patent Number 7,418,504 filed on July 1, 2013, Petitioner Apple Inc., – Exhibit 1005: Declaration of Chris Hopen, 25 pages (2013)	
	D1484	IPR2013-00393; Inter Partes Review of Patent Number 7,418,504 filed on July 1, 2013, Petitioner Apple Inc., – Exhibit 1006: Declaration of James Chester , 26 pages (2013)	
	D1485	IPR2013-00393; Inter Partes Review of Patent Number 7,418,504 filed on July 1, 2013, Petitioner Apple Inc., – Exhibit 1065: Yeager, Web Server Technology, 54 pages (1996)	
	D1486	IPR2013-00393; Inter Partes Review of Patent Number 7,418,504 filed on July 1, 2013, Petitioner Apple Inc., – Exhibit 1066: Microsoft Internet Explorer 5 Resource Kit, 21 pages (1999)	
	D1487	IPR2013-00393; Inter Partes Review of Patent Number 7,418,504 filed on July 1, 2013, Petitioner Apple Inc., – VirnetX Exhibit 2015: ITU-T Recommendation X.500, "Series Data Networks," 32 pages (2008)	
	D1488	IPR2013-00394; Inter Partes Review of Patent Number 7,418,504 filed on July 1, 2013, Petitioner Apple Inc., – Petition for Inter Partes Review of US Patent No 7,418,504, 73 pages	
	D1489	IPR2013-00394; Inter Partes Review of Patent Number 7,418,504 filed on July 1, 2013, Petitioner Apple Inc., - Exhibit 1003: Declaration of Michael Fratto, 203 pages (2013)	
	D1490	IPR2013-00394; Inter Partes Review of Patent Number 7,418,504 filed on July 1, 2013, Petitioner Apple Inc., - Exhibit 1005: Hopen Declaration, 25 pages (2013)	
	D1491	IPR2013-00394; Inter Partes Review of Patent Number 7,418,504 filed on July 1, 2013, Petitioner Apple Inc., - Exhibit 1006: Chester Declaration, 26 pages (2013)	
	D1492	IPR2013-00397; Inter Partes Review of Patent Number 7,921,211 filed on July 1, 2013, Petitioner Apple Inc., - Petition for Inter Partes Review, 63 pages (2013)	
	D1493	IPR2013-00397; Inter Partes Review of Patent Number 7,921,211 filed on July 1, 2013, Petitioner Apple Inc., - Exhibit 1003: Declaration of Michael Fratto, 184 pages (2013)	
	D1494	IPR2013-00397; Inter Partes Review of Patent Number 7,921,211 filed on July 1, 2013, Petitioner Apple Inc., - Exhibit 1005: Declaration of Chris Hopen, 25 pages (2013)	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1495	IPR2013-00397; Inter Partes Review of Patent Number 7,921,211 filed on July 1, 2013, Petitioner Apple Inc., - Exhibit 1006: Declaration of James Chester, 26 pages (2013)	
	D1496	IPR2013-00398; Inter Partes Review of Patent Number 7,921,211 filed on July 1, 2013, Petitioner Apple Inc., Petition for Inter Partes Review, 74 pages	
	D1497	IPR2013-00398; Inter Partes Review of Patent Number 7,921,211 filed on July 1, 2013, Petitioner Apple Inc., Exhibit 1003: Declaration of Michael Fratto regarding Patent Number 7,921,211, 204 pages (2013)	
	D1498	IPR2013-00398; Inter Partes Review of Patent Number 7,921,211 filed on July 1, 2013, Petitioner Apple Inc., Exhibit 1005: Declaration of Chris Hopen, 25 pages (2013)	
	D1499	IPR2013-00398; Inter Partes Review of Patent Number 7,921,211 filed on July 1, 2013, Petitioner Apple Inc., Exhibit 1006: Declaration of James Chester, 26 pages (2013)	
	D1500	IPR2014-00176; Inter Partes Review of Patent Number 7,418,504 filed on November 20, 2013, Petitioner RPX Corporation; Petition for Inter Partes Review, 60 pages	
	D1501	IPR2014-00176; Inter Partes Review of Patent Number 7,418,504 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1003; Declaration of Michael Fratto Regarding U.S. Patent Number 7,418,504, 242 pages (2013)	
	D1502	IPR2014-00176; Inter Partes Review of Patent Number 7,418,504 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1005; Declaration of Christ Hopen, 25 pages (2013)	
	D1503	IPR2014-00176; Inter Partes Review of Patent Number 7,418,504 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1006; Declaration of James Chester, 26 pages (2013)	
	D1504	IPR2014-00174; Inter Partes Review of Patent Number 7,418,504 filed on November 20, 2013, Petitioner RPX Corporation; Petition for Inter Partes Review, 60 pages	
	D1505	IPR2014-00174; Inter Partes Review of Patent Number 7,418,504 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1003: Declaration of Michael Fratto Regarding U.S. Patent Number 7,921,211, 242 pages (2013)	
	D1506	IPR2014-00174; Inter Partes Review of Patent Number 7,418,504 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1005: Declaration of Chris Hopen, 25 pages (2013)	
	D1507	IPR2014-00174; Inter Partes Review of Patent Number 7,418,504 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1006: Declaration of James Chester, 26 pages (2013)	
	D1508	IPR2014-00172; Inter Partes Review of Patent Number 6,502,135 filed on November 20, 2013, Petitioner RPX Corporation; Petition for Inter Partes Review, 67 pages	
	D1509	IPR2014-00172; Inter Partes Review of Patent Number 6,502,135 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1003:Declaration of Michael Fratto Regarding U.S. Patent Number 6,502,135, 196 pages (2013)	
	D1510	IPR2014-00172; Inter Partes Review of Patent Number 6,502,135 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1005: Declaration of Chris Hopen Regarding Prior Art and U.S. Patent Number 6,502,135, 25 pages (2013)	
	D1511	IPR2014-00172; Inter Partes Review of Patent Number 6,502,135 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1006: Declaration of James Chester, 26 pages (2013)	
	D1512	IPR2014-00171; Inter Partes Review of Patent Number 6,502,135 filed on November 20, 2013, Petitioner RPX Corporation; Petition for Inter Partes Review, 73 pages	
	D1513	IPR2014-00171; Inter Partes Review of Patent Number 6,502,135 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1003:Declaration of Michael Fratto Regarding U.S. Patent Number 6,502,135, 286 pages (2013)	
	D1514	IPR2014-00171; Inter Partes Review of Patent Number 6,502,135 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1005: Declaration of Chris Hopen Regarding Prior Art and U.S. Patent Number 6,502,135, 25 pages (2013)	
	D1515	IPR2014-00171; Inter Partes Review of Patent Number 6,502,135 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1006: Declaration of James Chester, 26 pages (2013)	
	D1516	IPR2014-00173; Inter Partes Review of Patent Number 7,490,151 filed on November 20, 2013, Petitioner RPX Corporation; Petition for Inter Partes Review, 72 pages	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** ***(Use as many sheets as necessary)***	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1517	IPR2014-00173; Inter Partes Review of Patent Number 7,490,151 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1003:Declaration of Michael Fratto Regarding U.S. Patent Number 6,502,135, 352 pages (2013)	
	D1518	IPR2014-00173; Inter Partes Review of Patent Number 7,490,151 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1005: Declaration of Chris Hopen Regarding Prior Art and U.S. Patent Number 7,490,151, 23 pages (2013)	
	D1519	IPR2014-00173; Inter Partes Review of Patent Number 7,490,151 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1006: Declaration of James Chester, 26 pages (2013)	
	D1520	IPR2014-00175; Inter Partes Review of Patent Number 7,921,211 filed on November 20, 2013, Petitioner RPX Corporation; Petition for Inter Partes Review, 66 pages	
	D1521	IPR2014-00175; Inter Partes Review of Patent Number 7,921,211 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1003:Declaration of Michael Fratto Regarding U.S. Patent Number 6,502,135, 209 pages (2013)	
	D1522	IPR2014-00175; Inter Partes Review of Patent Number 7,921,211 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1005: Declaration of Chris Hopen Regarding Prior Art and U.S. Patent Number 7,490,151, 25 pages (2013)	
	D1523	IPR2014-00175; Inter Partes Review of Patent Number 7,921,211 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1006: Declaration of James Chester, 26 pages (2013)	
	D1524	IPR2014-00177; Inter Partes Review of Patent Number 7,418,504 filed on November 20, 2013, Petitioner RPX Corporation; Petition for Inter Partes Review, 63 pages	
	D1525	IPR2014-00177; Inter Partes Review of Patent Number 7,418,504 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1003:Declaration of Michael Fratto Regarding U.S. Patent Number 6,502,135, 208 pages (2013)	
	D1526	IPR2014-00177; Inter Partes Review of Patent Number 7,418,504 filed on November 20, 2013, Apple Inc.; Exhibit 1005: Declaration of Chris Hopen Regarding Prior Art and U.S. Patent Number 7,490,151, 25 pages (2013)	
	D1527	IPR2014-00177; Inter Partes Review of Patent Number 7,418,504 filed on November 20, 2013, Apple Inc.; Exhibit 1006: Declaration of James Chester, 26 pages (2013)	
	D1528	IPR2014-00237; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc.; Petition for Inter Partes Review, 72 pages	
	D1529	IPR2014-00237; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc.; Exhibit 1003: Declaration of Michael Fratto Regarding U.S. Patent Number 8,504,697, 201 pages	
	D1530	IPR2014-00237; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc.; Exhibit 1015: Wedlund et al., "Mobility Support Using SIP,"pages 76-82 (1999)	
	D1531	IPR2014-00237; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Exhibit 1013: Schulzrinne et al., A Transport Protocol for Real-Time Applications, RFC 1889, 75 pages (1996)	
	D1532	IPR2014-00237; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Exhibit 1014: Handley et al., Session Description Protocol, RFC 2327,42 pages (1998)	
	D1533	IPR2014-00237; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Exhibit 1066: WAP Architecture Version 30, 20 pages (1998)	
	D1534	IPR2014-00237; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Exhibit 1067: World Wide Web Consortium and Wirelss Application Protocol Forum Establish Formal Liaison Relationship, 3 pages (1999)	
	D1535	IPR2014-00237; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Exhibit 1068: Data Over Cable Interface Specifications, 189 pages (1997)	
	D1536	IPR2014-00237; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Exhibit 1069: Nikolich, Cable Modems Deliver Fast Net Access, LexisNexis, 2 pages (1999)	
	D1537	IPR2014-00237; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Exhibit 1070: Duffy, Cabletron Enters Cable Modem Fray, LexisNexis, 2 pages (1998)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1538	IPR2014-00237; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Exhibit 1071: How it Works: Cable Modems, 2 pages (1999)	
	D1539	IPR2014-00237; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Exhibit 1072: Microsoft Press, Microsoft Computer Dictionary Fourth Edition, 9 pages (1999)	
	D1540	IPR2014-00237; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Exhibit 1075: IBM Session Initiation Protocol, 4 pages (2013)	
	D1541	IPR2014-00237; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Exhibit 1079: Shorter Oxford English Dictionary on Historical Principles, Fifth Edition, Volume 1 A-M, 3 pages (2002)	
	D1542	IPR2014-00238; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Petition for Inter Partes Review, 72 pages	
	D1543	IPR2014-00238; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Exhibit 1003: Declaration of Michael Fratto Regarding U.S. Patent Number 8,504,697, 240 pages (2013)	
	D1544	IPR2014-00238; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Exhibit 1005: Declaration of Chris Hopen Regarding Prior Art and U.S. Patent Number 7,490,151,23 pages (2013)	
	D1545	IPR2014-00238; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Exhibit 1006: Declaration of James Chester, 26 pages (2013)	
	D1546	IPR2014-00401; Inter Partes Review of Patent Number 7,188,180 filed on February 4, 2014, Petitioner Microsoft Corporation., – Petition for Inter Partes Review, 62 pages	
	D1547	IPR2014-00401; Inter Partes Review of Patent Number 7,188,180 filed on February 4, 2014, Petitioner Microsoft Corporation., - Exhibit 1005: Guillen et al., "An Architecture for Virtual Circuit/QoS Routing," Brussels University, 8 pages (1993)	
	D1548	IPR2014-00401; Inter Partes Review of Patent Number 7,188,180 filed on February 4, 2014, Petitioner Microsoft Corporation., - Exhibit 1006: Kosiur, "Building and Managing Virtual Private Networks," Wiley Computer Publishing, ISBN: 0471295264 (1998)	
	D1549	IPR2014-00401; Inter Partes Review of Patent Number 7,188,180 filed on February 4, 2014, Petitioner Microsoft Corporation., - Exhibit 1011: Guerin Declaration for 180 Patent (Provino) dated January 10, 2014	
	D1550	IPR2014-00401; Inter Partes Review of Patent Number 7,188,180 filed on February 4, 2014, Petitioner Microsoft Corporation., - Exhibit 1015: Redacted Settlement Agreement dated 5/14/2010	
	D1551	IPR2014-00403; Inter Partes Review of Patent Number 7,987,274 filed on February 4, 2014, Petitioner Microsoft Corporation., – Petition for Inter Partes Review, 58 pages	
	D1552	IPR2014-00403; Inter Partes Review of Patent Number 7,987,274 filed on February 4, 2014, Petitioner Microsoft Corporation., - Exhibit 1002: Excerpts from the Prosecution History of USP 7,987,274 filed 5/21/2013.	
	D1553	IPR2014-00404; Inter Partes Review of Patent Number 7,987,274 filed on February 4, 2014, Petitioner Microsoft Corporation., – Petition for Inter Partes Review, 58 pages	
	D1554	IPR2014-00404; Inter Partes Review of Patent Number 7,987,274 filed on February 4, 2014, Petitioner Microsoft Corporation., – Exhibit 1002: Excerpts from the Prosecution History of USP 7,987,274 dated 4/22/2013	
	D1555	IPR2014-00405; Inter Partes Review of Patent Number 7,987,274 filed on February 4, 2014, Petitioner Microsoft Corporation., – Petition for Inter Partes Review, 66 pages	
	D1556	IPR2014-00405; Inter Partes Review of Patent Number 7,987,274 filed on February 4, 2014, Petitioner Microsoft Corporation., - Exhibit 1012: Order of Dismissal dated 6/10/2010	
	D1557	IPR2014-00405; Inter Partes Review of Patent Number 7,987,274 filed on February 4, 2014, Petitioner Microsoft Corporation., - Exhibit 1013: Order of Dismissal dated 5/25/2010	
	D1558	IPR2014-00405; Inter Partes Review of Patent Number 7,987,274 filed on February 4, 2014, Petitioner Microsoft Corporation., Exhibit 1024: Excerpt from Prosecution History of Reexam 95/001,972	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1559	VirnetX v. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013, 43 pages	
	D1560	VirnetX v. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 37: SecureConnect vs. Claims of the '151 Patent, 4 pages	
	D1561	VirnetX v. Microsoft, Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 41: SFS-HTTP vs. Claims of the '151 Patent, 10 pages	
	D1562	VirnetX v. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 48: U.S. '132 vs. Claims of the '151 Patent, 15 pages	
	D1563	VirnetX v. Microsoft, Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 55: B&M VPNs vs. Claims of the '151 Patent, 12 pages	
	D1564	VirnetX v. Microsoft, Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 59: BorderManager vs. Claims of the '151 Patent, 18 pages	
	D1565	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 79: Valencia (019) vs. Claims of the '274 Patent, 12 pages	
	D1566	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 85: U.S. '748 vs. Claims of the '151 Patent, 8 pages	
	D1567	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 99: Araujo vs. Claims of the '135 Patent, 19 pages	
	D1568	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 100: Araujo vs. Claims of the "151 Patent, 8 pages	
	D1569	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 101: NetMeeting vs. Claims of the '135 Patent, 81 pages	
	D1570	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 102: NetMeeting vs. Claims of the '151 Patent, 53 pages	
	D1571	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 103: NetMeeting vs. Claims of the '180 Patent, 35 pages	
	D1572	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 104: NetMeeting vs. Claims of the '211 Patent, 47 pages	
	D1573	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 105: NetMeeting vs. Claims of the '274 Patent, 26 pages	
	D1574	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 106: NetMeeting vs. Claims of the '504 Patent, 48 pages	
	D1575	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 107: EverLink vs. Claims of the '151 Patent, 39 pages	
	D1576	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 108: Special Anthology vs. Claims of the '135 Patent, 4 pages	
	D1577	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 109: Gauntlet for IRIX vs. Claims of the '135 Patent, 62 pages	
	D1578	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 110: Gauntlet for IRIX vs. Claims of the '211 Patent, 111 pages	
	D1579	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 111: Gauntlet for IRIX vs. Claims of the '504 Patent, 119 pages	
	D1580	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 112: Gauntlet System vs. Claims of the '135 Patent, 24 pages	
	D1581	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 113: Gauntlet System vs. Claims of the '151 Patent, 23 pages	
	D1582	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 108: Gauntlet System vs. Claims of the '180 Patent, 36 pages	
	D1583	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 115: Gauntlet System vs. Claims of the '211 Patent, 67 pages	
	D1584	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 116: Gauntlet Systems vs. Claims of the '504 Patent, 69 pages	
	D1585	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 117: Gauntlet Systems vs. Claims of the '274 Patent, 16 pages	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1586	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 123: IntraPort System vs. Claims of the '274 Patent, 24 pages	
	D1587	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 129: Overview vs. Claims of the '274 Patent, 12 pages	
	D1588	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 135: Schulzrinne vs. Claims of the '274 Patent, 14 pages	
	D1589	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 141: Solana vs. Claims of the '274 Patent, 17 pages	
	D1590	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 147: Atkinson vs. Claims of the '274 Patent, 15 pages	
	D1591	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 153: Marino vs. Claims of the '274 Patent, 11 pages	
	D1592	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 159: Valencia (213) vs. Claims of the '274 Patent, 13 pages	
	D1593	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 166: Davison vs. Claims of the '274 Patent, 11 pages	
	D1594	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 170: AutoSOCKS vs. Claims of the '274 Patent, 14 pages	
	D1595	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 174: Aventail Connect 3.01/2.51 vs. Claims of the '274 Patent, 17 pages	
	D1596	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 176: Aventail Connect 3.1/2.6 Administrator's Guide("Aventail Connect") vs. Claims of the '211 Patent, 56 pages	
	D1597	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 179: Aventail Connect 3.1/2.6 vs. Claims of the '274 Patent, 19 pages	
	D1598	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 183: BinGO! User's Guide/Extended Features Reference vs. Claims of the '274 Patent, 26 pages	
	D1599	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 210: Cisco's Prior Art Systems vs. Claims of the '274 Patent, 19 pages	
	D1600	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 213: Cisco's Prior Art PIX System vs. Claims of the '151 Patent, 37 pages	
	D1601	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 214: Cisco's Prior Art PIX System vs. Claims of the '211 Patent, 104 pages	
	D1602	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 244: Understanding OSF DCE 1.1 for AIX and OS/2 (APP_VX0556531-804) vs. Claims of the '274 Patent, 26 pages	
	D1603	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 228: Abadi vs. Claims of the '135 Patent, 12 pages	
	D1604	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 229: Abadi vs. Claims of the '180 Patent, 16 pages	
	D1605	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 230: Abadi vs. Claims of the '151 Patent, 10 pages	
	D1606	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 231: Abadi vs. Claims of the '274 Patent, 11 pages	
	D1607	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 237: Kiuchi vs. Claims of the '274 Patent, 30 pages	
	D1608	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 243: Aziz vs. Claims of the '274 Patent, 37 pages	
	D1609	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 248: RFC 2543 vs. Claims of the '180 Patent, 48 pages	
	D1610	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 249: RFC 2543 vs. Claims of the '274 Patent, 28 pages	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** ***(Use as many sheets as necessary)***	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1611	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 252: Wesinger vs. Claims of the '180 Patent, 42 pages	
	D1612	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 253: Wesinger vs. Claims of the '274 Patent, 23 pages	
	D1613	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 257: Provino vs. Claims of the '180 Patent, 17 pages	
	D1614	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 258: U.S. Patent Number 6,557,037 vs. Claims of the '504 Patent, 17 pages	
	D1615	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 259: Provino vs. Claims of the '151 Patent, 13 pages	
	D1616	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 261: Provino vs. Claims of the '274 Patent, 15 pages	
	D1617	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 262: NT4 System vs. Claims of the '135 Patent, 22 pages	
	D1618	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 263: NT4 System vs. Claims of the '151 Patent, 12 pages	
	D1619	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 264: EverLink vs. Claims of the '274 Patent, 38 pages	
	D1620	New Version of Windows 98 Improves the Business of Running a Home; Windows 98 Second Edition Makes it Easier for Families to Connect, June 10, 1999	
	D1621	Research Advances in Database and Information Systems Security, Kluwer Academic Publishers, July 25-28 (1999)	
	D1622	Barkley et al., "Role Based Access Control for the World Wide Web," Abstract, pages 1-11, April 8 (1997)	
	D1623	Abadi et al., "Secure Web Tunneling," Computer Networks and ISDN Systems, 30:531-539 (1998)	
	D1624	Communications and Multimedia Security II; Proceedings of the IFIP TC6/TC11 International Conference on Communications and Multimedia Security at Essen, Germany, September 23-24 (1996)	
	D1625	IEEE Computer Society, Seventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE '98); June 17-19 (1998)	
	D1626	Kahan, "WDAI: A Simple World Wide Web Distributed Authorization Infrastructure," Computer Networks, 31:1599-1609 (1999)	
	D1627	Norifusa, "Internet Security: Difficulties and Solutions," International Journal of Medical, 49:69-74 (1998)	
	D1628	Molva, "Internet Security Architecture," 31:787-804 (1999)	
	D1629	Ellermann, "IPv6 and Firewalls," June 1996	
	D1630	Herscovitz, "Secure Virtual Private Networks: The Future of Data Communications," International Journal of Network Management, 9:213-220 (1999)	
	D1631	Cheswick et al., "A DNS Filter and Switch for Packet-Filtering Gateways," Proceedings of the Sixth USENIX UNIX Security Symposium, 1996	
	D1632	Farrow, "How DNS Can Divulge Sensitive Information," Network Magazine, 14(3):72 (1999)	
	D1633	Greenwald et al., "Designing an Academic Firewall: Policy, Practice, and Experience with SURF," Proceedings of the SNDSS, 1996	
	D1634	Collins, "Designing Secure Intranets," Computing & Control Engineering Journal, pages 185-192, 1998	
	D1635	Lioy et al., "DNS Security," Terena Networking Conference, pages 1-13, May 22-25 (2000)	
	D1636	Davidowicz, "Domain Name System (DNS) Security," pages 1-22, (1999)	
	D1637	Gilmore et al., "Secure Remote Access to an Internal Web Server," IEEE Network, pages 31-37 (1999)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** ***(Use as many sheets as necessary)***	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1638	Using NETBuilder Family Software, Version 11.0, Published March 1998, http://www.3com.com/	
	D1639	AccessBuilder 2000/4000/5000 Server Configuration Guide, Software Version 7.0, Published April 1997, http://www.3com.com/	
	D1640	Apple Remote Access 3.0, Apple Remote Access Client and Apple Remote Access Personal Server User's Manual (1997)	
	D1641	Macaire et al., "A Personal Naming and Directory Service for Mobile Internet Users," USENIX Workshop on Smartcard Technology, May 10-11 (1999)	
	D1642	Sidewinder Network Gateway Security, Administration Guide Version 7.0, Secure Computing Corporation, 812 pages (2007)	
	D1643	Zao et al., "Domain Based Internet Security Policy Management," pages 41-53 (1999)	
	D1644	Aventail and Spyrus Join Forces to Deliver High-Assurance Extranet Security Solutions for the Enterprise, Business Wire, May 12, 1999	
	D1645	Aventail Ships Directory-Enabled Extranet Solution; Aventail Extranet Center V3.1 Available at www.aventail.com, Business Wire, August 9, 1999	
	D1646	Mooi Choo Chuah et al., "Mobile Virtual Private Dial-Up Services," Bell Labs Technical Journal, (1999)	
	D1647	The Brick Extended Features Reference.Manual, 288 pages (1999)	
	D1648	Bianca/Brick Software Reference Manual, Version 2.3, 331 pages (1999)	
	D1649	Bianca/Brick Software Reference Manual, Version 2.4, (1999)	
	D1650	Novell BorderManager; Installation and Setup, Version 3.5, 162 pages (1999)	
	D1651	Broadband Forum Technical Support, Core Network Architecture Recommendations for Access to Legacy Data Networks Over ADSL, Issue 1.0, 24 pages (1999)	
	D1652	Cabletron Routing Software; Routing Protocols Reference Guide, Cabletron Systems (1999)	
	D1653	Cisco Systems, Virtual Private Networks (VPN), Internetworking Technical Overview, (1999)	
	D1654	Cisco Systems, Cisco Access Product Family, 16 pages (1996)	
	D1655	Cisco, MPLS Virtual Private Networks, (1999)	
	D1656	WEBDAV: Distributed Authoring and Versioning Presentation vs. Greg Stein, Adobe Technical Seminar Series, May, 1999	
	D1657	Valencia et al., "Layer Two Tunneling Protocol "LSTP"," Internet Draft (1998)	
	D1658	Patel, "Securing L2TP Using IPSEC," Internet Draft (1999)	
	D1659	Srisuresh, "Secure Remote Access with L2TP," Internet Draft (1999)	
	D1660	IBM Corporation, AS/400 TCP/IP Autoconfiguration DNS and DHCP Support, 457 pages (1998) available at http://www.redbooks.ibm.com	
	D1661	IBM Corporation, Inside the VPN Tunnel, IBM Technical Support, 23 pages (1999)	
	D1662	IBM Corporation, IBM Firewall for AS/400 V4R3: VPN and NAT Support, 361 pages (1999)	
	D1663	IBM Corporation, Software User's Guide, Version 3.2, (1998)	
	D1664	IBM Corporation, Software User's Guide Version 3.3, 678 pages (1999)	
	D1665	IBM Corporation, Using and Configuring Features, Version 3.2, 336 pages, (1998)	
	D1666	IBM Corporation, Software User's Guide, Version 3.4, 770 pages (1999)	
	D1667	IBM Corporation, A Comprehensive Guide to Virtual Private Networks, Volume I: IBM Firewall, Server and Client Solutions, 36 pages (1998) available at http://www.redbooks.ibm.com	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1668	IBM Corporation, A Comprehensive Guide to Virtual Private Networks, Volume II: IBM Nways Router Solutions, 622 pages (1999) available at http://www.redbooks.ibm.com	
	D1669	IBM Corporation, A Comprehensive Guide to Virtual Private Networks, Volume III: Cross-Platform Key and Policy Management, 665 pages (1999) available at http://www.redbooks.ibm.com	
	D1670	Novell, BorderManager, Overview and Planning, Enterprise Edition 3, Version 3.5 (1999)	
	D1671	Zyxel Total Intemet Access Solution; User's Guide, Version 2.20 (1999)	
	D1672	Raptor Integrated Enterprise Network Security System V6.0; Raptor Firewall Reference Guide (1998)	
	D1673	Reynolds et al., "Assigned Numbers," RFC 1700 (1994)	
	D1674	Blake et al., "An Architecture for Differentiated Services," RFC 2475 (1998)	
	D1675	Aboba et al., "The Network Access Identifier," RFC 2486 (1999)	
	D1676	Rosen et al., "BGP/MPLS VPNs, RFC 2547 (1999)	
	D1677	Pall et al., "Microsoft Point-To-Point Encryption (MPPE) Protocol," RFC 3078 (2001)	
	D1678	Cisco Systems, Release Notes for the Cisco Secure VPN Client Versions 1.0/1.0a (1999)	
	D1679	Ascend Communications, Inc., SecureConnect Manager User's Guide (1998)	
	D1680	Kaminsky et al., "SFS-HTTP: Securing the Web with Self-Certifying URLs," (1999) available at http://www.pdos.lcs.mit.edu/"kaminsky/sfs-http.ps	
	D1681	Timestep Corporation, Understanding the IPSec Protocol Suite (1998)	
	D1682	Level One, Level One User Manual (1999)	
	D1683	Stein et al., "Writing Apache Modules with Perl and C," ISBN:1-56592-567, 746 pages (1999)	
	D1684	Shea, "L2TP Implementation and Operation," The Addison-Wesley Networking Basics Series (2000)	
	D1685	McCormack et al., "An Authentication Framework for Web Access to Remote Hosts," National Institute of Standards and Technology (1998)	
	D1686	Harney et al., "Group Key Management Protocol (GKMP) Architecture," RFC 2094 (1997)	
	D1687	Sijben et al., "Bridging the Gap to IP Telephony," Bell Labs Technical Journal (1998)	
	D1688	Hoffman, "SMTP Service Extension for Secure SMTP over TLS," RFC 2487 (1999)	
	D1689	Newman, "Using TLS with IMAP, POP3 and ACAP," RFC 2595 (1999)	
	D1690	Using Internet VPN to Bring Job Sites and Branch Offices Online, Nikkei Communications (1997)	
	D1691	ANX CEP Interconnection Options, Bellcore/ANXO, October 1, 1998	
	D1692	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Atkinson, "An Internetwork Authentication Architecture," Naval Research Laboratory, Center for High Assurance Computing Systems (8/5/93)	
	D1693	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Eastlake, Domain Name System Security Extensions, IETF DNS Security Working Group (December 1998), available at http://www.watersprins.org/pub/id/draft-ietf-dnssec-secext2-07.txt	
	D1694	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Goldschlag et al., "Privacy on the Internet," Naval Research Laboratory, Center for High Assurance Computer Systems (1997)	
	D1695	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Goldschlag et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK (May 1996)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1696	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Goldschlag et al., "Onion Routing for Anonymous and Private Internet Connection," Naval Research Laboratory, Center for High Assurance Computer Systems (January 28, 1999)	
	D1697	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. M.G. Reed et al., "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA December 9-13 1996	
	D1698	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Macdonald et al., "PF_KEY key Management API, Version 2," Network Working Group, RFC 2367 (July 1998) ("RFC 2367")	
	D1699	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Onion Routing, "Investigation of Route Selection Algorithms," available at http://www.onion-router.net/Archives/Route/index.html ("Route Selection")	
	D1700	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Scott et al., Virtual Private Networks, O'Reilly and Associates, Inc., 2nd ed (Jan. 1999) ("Scott VPNs')	
	D1701	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Syverson et al., "Private Web Browsing," Naval Research Laboratory, Center for High Assurance Computer Systems (June 2, 1997) ("Syverson")	
	D1702	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. "IPSec Minutes From Montreal," IPSEC Working Group Meeting Notes, http://www.sandleman,ca/ipsec/1996/08/msg00018.html (June 1996)	
	D1703	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. "Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources," FirstVPN, (Jan 2000) ("First VPN Building a Microsoft VPN Publication")	
	D1704	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Publicly Available DNS-Related Correspondence dated September 7, 1993 to September 20, 1993 ("DNS-Related Correspondence")	
	D1705	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Assured Digital Incorporated Products ("ADI Products")	
	D1706	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. DNS SRV references (1996, 1998, 1999, 2000)	
	D1707	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. U.S. Patent Number 5,898,830 ("Wesinger '830 Patent")	
	D1708	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Global VPN ("GVPN") references (1999)	
	D1709	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Kaufman et al., Implementing IPsec: Making Security Work on VPNs, Intranets, and Extranets, (Copyright 1999) ("Implementing IPsec")	
	D1710	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Safe Surfing: How to Build a Secure World Wide Web Connection, IBM Int'l Technical Support Organization (March 1996) ("Safe Surfing")	
	D1711	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. U.S. Provision Patent Application No. 60/134,547 (filed May 17, 1999) ("Sheymov")	
	D1712	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Data Fellows F-Secure VPN ("F-Secure VPN+ Publication")	
	D1713	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. U.S. Pat. No. 5,950,195 ("Stockwell '195 Patent")	
	D1714	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. B. Patel et al., "DHCP Configuration of IPSEC Tunnel Mode," IPSEC Working Group, Internet Draft 02 (10/15/1999) ("Patel")	
	D1715	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. SSL VPNs ("SSL VPNs") references (1996, 1997, 1998)	
	D1716	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Gauntlet Firewall ("Gauntlet FW") references (1995, 1996, 1999)	
	D1717	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. U.S. Pat. No. 6,119,171 ("'171 patent")	
	D1718	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Caronni et al., U.S. Patent No. 5,822,434 October 13, 1998 (filed June 18, 1996) ("'434 patent)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	Complete if Known	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1719	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. RFC 2230 (November 1997) U.S. Patent No. 5,511,122 (April 23, 1996)	
	D1720	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Check Point FW as described in: Goncalves et al., Check Point Firewall -1 Administration Guide, McGraw-Hill Companies (2000) available at http://www.books24x7.com/book/id 762/viewer r.asp?bookid=762&chunkid=410651062 (Goncalves, Check Point FW); Check Point Software Technologies Ltd. (1999) (Check Point FW)	
	D1721	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. CIS/DCOM as described in: Microsoft Corp., Cariplo: Distributed Component Object Model, references (1996-1999)	
	D1722	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Bhattacharya et al., "An LDAP Schema for Configuration and Administration of IPSec Based Virtual Private Networks (VPNs)", IETF Internet Draft (October 1999) ("LDAP Schema for IPSec based VPNs publication")	
	D1723	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Onion Routing references (1996, 1997, 1999	
	D1724	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Aventail references (1997-1999)	
	D1725	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. C. Huitema et al., "Simple Gateway Control Protocol," Version 1.0 (May 5, 1998) ("SGCP")	
	D1726	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. Microsoft VPN Technology references (1997-1999)	
	D1727	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. Dynamic VPN ("DVPN") references (1997-2001)	
	D1728	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. R.G. Moskowitz, "Network Address Translation Issues with IPsec," Internet Draft, Internet Engineering Task Force, February 6, 1998 ("Moskowitz")	
	D1729	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. F-Secure VPN and F-Secure VPN references (1996, 1998, 1999)	
	D1730	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. Atkinson et al., "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998) ("RFC 2401")	
	D1731	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. RFC 2543 and Internet Drafts (1999)	
	D1732	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. AltaVista Tunnel and/or the AltaVista Firewall references (1997, 1998)	
	D1733	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. Henning Schulzrinne, Personal Mobility for Multimedia Services in the Internet, Proceedings of the European Workshop on Interactive Distributed Multimedia Systems and Services (1996) ("Schulzrinne 96")	
	D1734	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. Schulzrinne U.S. Pat. No. 6,937,597 (August 30, 2005)	
	D1735	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. J.M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California (July 1996) ("Galvin")	
	D1736	Microsoft Claim Chart of U.S. Patent No. 6,502, 135; vs. Naganand Doraswamy, Implementation of Virtual Private Network (VPNs) with IP Secrity [sic] <draft-ietf-ipsec-vpn-00.txt> (March 12, 1997) ("Doraswamy")	
	D1737	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. FreeS/WAN references (1996)	
	D1738	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. 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"); J. Gilmore et al., Re: Key Management, anyone? (DNS keying) IETF IPSec Working Group Mailing List Archive (8/96 - 9/96)	
	D1739	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. the Automotive Network exchange ("ANX) references (1997, 1999)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1740	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. The Defense Information Systems Agency, Secret Internet Protocol router Network (SIPRNET)[1] references (1998, 2000)	
	D1741	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. U.S. Patent Application No. 09/399,753 ("the Miller Application") as published in U.S. Pub. No. 2005/0055306 (Priority Date: 09/22/98)	
	D1742	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. R. Atkinson, "An Internetwork Authentication Architecture," Naval Research Laboratory, Center for High Assurance Computing Systems (8/5/93) ("Atkinson NRL")	
	D1743	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Donald Eastlake, Domain Name System Security Extensions, IETF DNS Security Working Group (December 1998), available at http://www.watersprings.org/pub/id/draft-ietf-dnssec-secext2-07.txt ("DNSSEC-7")	
	D1744	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Goldschlag et al., "Privacy on the Internet," Naval Research Laboratory, Center for High Assurance Computer Systems (1997) ("Goldschlag I")	
	D1745	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Goldschlag et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK (May 1996) ("Goldschlag II")	
	D1746	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Goldschlag et al., "Onion Routing for Anonymous and Private Internet Connection," Naval Research Laboratory, Center for High Assurance Computer Systems (January 28, 1999) ("Goldschlag III)	
	D1747	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. M.G. Reed, et al., "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA Dec. 9-13, 1996 ("Reed")	
	D1748	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. D. MacDonald et al., "PF_KEY Key Management API, Version 2," Network Working Group, RFC 2367 (July 1998) ("RFC 2367")	
	D1749	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Onion Routing, "Investigation of Route Selection Algorithms," available at http://www.onion-router.net/Archives/Route/index.html ("Route Selection")	
	D1750	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Scott et al., Virtual Private Networks, O'Reilly and Associates, Inc., 2nd ed. (Jan. 1999) ("Scott VPNs")	
	D1751	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Syverson et al., "Private Web Browsing," Naval Research Laboratory, Center for High Assurance Computer Systems (June 2, 1997) ("Syverson")	
	D1752	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. SafeNet VPN Products ("SafeNet VPN Products,") (1999-2000)	
	D1753	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. "Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources," FirstVPN, (Jan 2000) ("First VPN Building a Microsoft VPN publication")	
	D1754	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Publicly Available DNS-Related Correspondence dated September 7, 1993 to September 20, 1993 ("DNS-related Correspondence")	
	D1755	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. DNS SRV references (1996, 1998, 1999, 2000)	
	D1756	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. U.S. Pat. No. 5,898,830 ("Wesinger '830 Patent")	
	D1757	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Global VPN references (1999)	
	D1758	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Kaufman et al., Implementing IPsec: Making Security Work on VPNs, Intranets, and Extranets, (Copyright 1999) ("Implementing IPsec")	

[1] SIPRNET is a U.S. Government Internet Protocol network for the transport of information classified as SECRET. SIPRNET was built starting in 1995, and contains domain names bearing the ".smil" designation. Microsoft has subpoenaed information from the Department of Defense and others relationg to SIPRNET, and reserves the right to amend its contentions to take any additional information about SIPRNET that it receives into account.Department of Defense and others relationg to SIPRNET, and reserves the right to amend its contentions to take any additional information about SIPRNET that it receives into account.

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** ***(Use as many sheets as necessary)***	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1759	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. PGP Security, Finding Your Way Through the VPN Maze (1999) ("PGP")	
	D1760	Microsoft Claim Chart of U.S. Patent No. 6,839,759); vs. Safe Surfing: How to Build a Secure World Wide Web Connection, IBM Int'l Technical Support Organization (March 1996) ("Safe Surfing")	
	D1761	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. U.S. Provisional Patent Application No. 60/134,547 (filed May 17,1999) ("Sheymov")	
	D1762	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Data Fellows·F-Secure VPN ("F-Secure VPN+ Publication")	
	D1763	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. U.S. Pat. No. 5,950,195 ("Stockwell '195 Patent'")	
	D1764	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. B. Patel et al., "DHCP Configuration of IPSEC Tunnel Mode, "IPSEC Working Group, Internet Draft 02 (10/15/1999) ("Patel")	
	D1765	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. SSL VPNs ("SSL VPNs") references (1996-1997)	
	D1766	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Gauntlet Firewall ("Gauntlet FW") references (19995, 1996, 1999)	
	D1767	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Caronni et al., U.S. Patent No. 5,822,434 October 13, 1998 (filed June 18, 1996) ("'434 patent)	
	D1768	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. U.S. Pat. No. 5,311,593 ("'593 patent")	
	D1769	Microsoft Claim Chart of U.S. Patent No. 6,839,759; RFC 2230 (November 1997) U.S. Pat. No. 5,511,122 (April 23, 1996)	
	D1770	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Check Point FW as described in: Goncalves et al., Check Point FireWall-1 Administration Guide, McGraw-Hill Companies (2000) available at http://www.books24x7.com/book/id_762/viewer_r.asp?bookid=762&chunkid=410651062 (Goncalves, Check Point FW); Check Point Software Technologies Ltd. (1999) (Checkpoint FW)	
	D1771	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. CIS/DCOM references (1996, 1997, 1998, 1999)	
	D1772	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Bhattacharya et al., "An LDAP Schema for Configuration and Administration of IPSec Based Virtual Private Networks (VPNs)", IETF Internet Draft (October 1999) ("LDAP Schema for IPSec based VPNs publication")	
	D1773	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Onion Routing references (1996, 1997, 1999)	
	D1774	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Aventail references (1996, 1997, 1999)	
	D1775	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. C. Huitema et al., "Simple Gateway Control Protocol," Version 1.0 (May 5, 1998) ("SGCP")	
	D1776	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Microsoft VPN Technology references (1997-1999)	
	D1777	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Dynamic VPN ("DVPN") references (1997-2001)	
	D1778	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. R.G. Moskowitz, "Network Address Translation Issues with IPsec," Internet Draft, Internet Engineering Task Force, February 6, 1998 ("Moskowitz")	
	D1779	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Ted Harwood, Windows NT Terminal Server and Citrix MetaFrame (New Riders 1999) ("Windows NT Harwood")	
	D1780	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Todd W. Mathers and Shawn P. Genoway, Windows NT Thin Client Solutions: Implementing Terminal Server and Citrix MetaFrame (Macmillan Technical Publishing 1999) ("Windows NT Mathers")	
	D1781	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. F-Secure VPN and F-Secure VPN+ references (1996-1999)	
	D1782	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. TimeStep, "The Business Case for Secure VPNs" (1998) ("TimeStep")	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1783	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Atkinson et al., "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998) ("RFC 2401")	
	D1784	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. U.S. Pat. No. 6,079,020 ("VPNet '020 Patent")	
	D1785	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. U.S. Pat. No. 6,173,399 ("VPNet '399 Patent")	
	D1786	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. U.S. Pat. No. 6,226,748 ("VPNet '748 Patent")	
	D1787	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. U.S. Pat. No. 6,226,751 ("VPNet '751 Patent")	
	D1788	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Aboba et al., "Securing L2TP using IPSEC," PPPEXT Working Group, Internet Draft (February 2, 1999) ("L2TP/IPSEC")	
	D1789	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. AltaVista Tunnel and/or the AltaVista Firewall references (1997, 1998)	
	D1790	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Henning Schulzrinne, Personal Mobility for Multimedia Services in the Internet, Proceedings of the European Workshop on Interactive Distributed Multimedia Systems and Services (1996) ("Schulzrinne 96")	
	D1791	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. U.S. Pat. No. 6,701,437 ("VPNet '437 Patent")	
	D1792	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. WatchGuard references (2000)	
	D1793	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. J.M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California (July 1996) ("Galvin")	
	D1794	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Naganand Doraswamy, Implementation of Virtual Private Network (VPNs) with IP Secrity [sic.] <draft-ietf-ipsec-vpn-00.txt> (March 12, 1997) ("Doraswamy")	
	D1795	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. FreeS/WAN references (1996)	
	D1796	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. 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"); J. Gilmore et al., Re: Key Management, anyone? (DNS keying) IETF IPSec Working Group Mailing List Archive (8/96 – 9/96)	
	D1797	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. The Defense Information Systems Agency, Secret Internet Protocol Router Network (SIPRNET) references (1998, 2000)	
	D1798	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Donald Eastlake, Domain Name System Security Extensions, IETF DNS Security Working Group (December 1998), available at http://www.watersprings.org/pub/id/draft-ietf-dnssec-secext2-07/txt ("DNSSEC-7")	
	D1799	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Goldschlag et al., "Privacy on the Internet," Naval Research Laboratory, Center for High Assurance Computer Systems (1997) ("Goldschlag I")	
	D1800	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Goldschlag et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK (May 1996) ("Goldschlag II")	
	D1801	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Goldschlag et al., "Onion Routing for Anonymous and Private Internet Connection," Naval Research Laboratory, Center for High Assurance Computer Systems (January 28, 1999) ("Goldschlag III")	
	D1802	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. M.G. Reed, et al. "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA Dec. 9-13, 1996 ("Reed")	
	D1803	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. D. McDonald et al., "PF_KEY Key Management API, Version 2," Network Working Group, RFC 2367 (July 1998) ("RFC 2367")	
	D1804	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Onion Routing, "Investigation of Route Selection Algorithms," available at http://www.onion-router.net/Archives/Route/index.html ("Route Selection")	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1805	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Scott et al., Virtual Private Networks, O'Reilly and Associates, Inc., 2nd ed. (Jan. 1999) ("Scott VPNs")	
	D1806	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Syverson et al., "Private Web Browsing," Naval Research Laboratory, Center of High Assurance Computer Systems (June 2, 1997) ("Syverson")	
	D1807	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. "IPSec Minutes from Montreal," IPSEC Working Group Meeting Notes, http://sandleman.ca/ipsec/1996/08/msg00018.html (June 1996)	
	D1808	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. "Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources," FirstVPN, (Jan 2000) ("First VPN Building a Microsoft VPN publication")	
	D1809	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. DNS SRV references (1996, 1998, 1999, 2000)	
	D1810	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. U.S. Pat. No. 5,898,830 ("Wesigner '830 Patent")	
	D1811	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Kaufman et al., Implementing IPsec: Making Security Work on VPNS, Intranets, and Extranets (Copyright 1999) ("Implementing IPsec")	
	D1812	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Safe Surfing: How to Build a Secure World Wide Web Connection, IBM Int'l Technical Support Organization (March 1996) ("Safe Surfing")	
	D1813	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. U.S. Provisional Patent Application No. 60/134,547 (filed May 17, 1999) ("Sheymov")	
	D1814	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Data Fellows F-Secure VPN ("F-Secure VPN+ Publication)	
	D1815	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. U.S. Pat. No. 5,950,195 ("Stockwell '195 Patent")	
	D1816	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. B. Patel et al., "DHCP Configuration of IPSEC Tunnel Mode," IPSEC Working Group, Internet Draft 02 (10/15/1999) ("Patel")	
	D1817	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. SSL VPNs ("SSL VPNs") references (1996, 1999)	
	D1818	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Gauntlet Firewall ("Gauntlet FW") references (1995, 1996, 1999)	
	D1819	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. U.S. Pat. No. 6,199,171 ("'171 patent")	
	D1820	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Caronni et al., U.S. Patent No. 5,822,434 October 13, 1998 (filed June 18, 1996) ("'434 patent")	
	D1821	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. U.S. Pat. No. 6,005,574 ("'574 patent")	
	D1822	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. RFC 2230 (November 1997) ("KX Records"); U.S. Pat. No. 5,511,122 (April 23, 1996)	
	D1823	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Check Point FW as described in: Goncalves et al., Check Point FireWall -1 Administration Guide, McGraw-Hill Companies (2000) available at http://www.books24x7.com/book/id_762/viewer_r.asp?bookid=762&chunkid=410651062 (Goncalves, Check Point FW); Check Point Software Technologies Ltd. (1999) (Checkpoint FW)	
	D1824	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Battacharya et al., "An LDAP Schema for Configuration and Administration of IPSec Based Virtual Private Networks (VPNs)", IETF Internet Draft (October 1999) ("LDAP Schema for IPSec based VPNs publication")	
	D1825	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Onion Routing references (1996, 1997, 1999)	
	D1826	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Aventail references (1997, 1999)	
	D1827	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Microsoft VPN Technology references (1997-1999)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1828	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. R.G. Moskowitz, "Network Address Translation Issues with IPsec," Internet Draft, Internet Engineering Task Force, February 6, 1998 ("Moskowitz")	
	D1829	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. RFC 2543 and Internet Drafts (1999)	
	D1830	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. AltaVista Tunnel and/or the AltaVista Firewall references (1997); Birrell et al., U.S. Pat. No. 5,805,803, Sep. 8, 1998 (filed May 13, 1997)	
	D1831	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Henning Schulzrinne, Personal Mobility for Multimedia Services in the Internet, Proceedings of the European Workshop on Interactive Distributed Multimedia Systems and Services (1996) ("Schulzrinne 96")	
	D1832	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. J. M. Gavin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California (July 1996) ("Galvin")	
	D1833	Microsoft Claim Chart of U.S. Patent No. 7,188,180; Naganand Doraswamy, Implementation of Virtual Private Networks (VPNs) with IP Secrity [sic.] <draft-ietf-ipsec-vpn-00.txt> (March 12, 1997) ("Doraswamy")	
	D1834	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. FreeS/WAN references (1996)	
	D1835	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. H. Orman et al., Re: 'Re: DNS? Was Re: Key Management, anyone?, IETF IPSec Working Group Mailing List Archive (9/96 – 9/96) ("Orman DNS"); J. Gilmore et al., Re: Key Management, anyone? (DNS keying) IETF IPSec Working Group Mailing List Archive (8/96 - 9/96)	
	D1836	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. The Defense Information Systems Agency, Secret Internet Protocol Router Network (SIPRNET) references (1998, 2000)	
	D1837	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Dynamic VPN ("DVPN") reference (1997-2001)	
	D1838	Pereira, "Extended Authentication Within ISAKMP/Oakley," IP Security Working Group, Internet Draft (1998)	
	D1839	Patel et al., "Revised SA Negotiation Mode for ISAKMP/Oakley," IP Security Working Group, Internet Draft (1997)	
	D1840	Pereira et al., "The ISAKMP Configuration Method," IP Security Working Group (1998)	
	D1841	Piper, "A GSS-API Authentication Mode for ISAKMP/Oakley," Internet Draft (1997)	
	D1842	Rescorla, "HTTP Over TLS," Internet Draft (1999)	
	D1843	Lottor, "Domain Administrators Operations Guide," RFC 1033 (1987)	
	D1844	Everhart et al., "New DNS RR Definitions," RFC 1183 (1990)	
	D1845	Hardcastle-Kille, "X.500 and Domains, RFC 1279 (1991)	
	D1846	Manning, "DNS NSAP RRS," RFC 1348 (1992)	
	D1847	Huitema, "An Experiment in DNS Based IP Routing," RFC 1383 (1992)	
	D1848	Eastlake, "Physical Link Security Type of Service," RFC 1455 (1993)	
	D1849	Housley, "Security Label Framework for the Internet," RFC ":1457 (1993)	
	D1850	Kastenholz, "The Definitions of Managed Objects for the Security Protocols of the Point to Point Protocol," RFC 1472 (1993)	
	D1851	Kaufman, "DASS Distribution Authentication Security Service," RFC 1507 (1993)	
	D1852	Linn, "Generic Security Service Application Program Interface," RFC 1508 (1993)	
	D1853	Wray, "Generic Security Service API: C-Bindings, RFC 1509 (1993)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1854	Postel, "Domain Name System Structure and Delegation," RFC 1591 (1994)	
	D1855	Austein et al., "DNS Server MIB Extension," RFC 1611 (1994)	
	D1856	Austein et al., "DNS Resolver MIB Extensions," RFC 1612 (1994)	
	D1857	Manning et al., "DNS NSAP Resource Records," RFC 1637 (1994)	
	D1858	Allocchio et al., "Using the Internet DNS to Distribute RFC 1327 Mail Address Mapping Tables," RFC 1664 (1994)	
	D1859	Manning et al., "DNS NSAP Resource Records," RFC 1706 (1994)	
	D1860	Farrell et al., "DNS Encoding of Geographical Location," RFC 1712 (1994)	
	D1861	Brisco, "DNS Support for Load Balancing," RFC 1794 (1995)	
	D1862	Atkinson, "IP Authentication Header, RFC 1826 (1995)	
	D1863	Atkinson, "IP Encapsulating Security Payload (ESP)," RFC 1827 (1995)	
	D1864	Metzger, "IP Authentication Using Keyed MDS," RFC 1828 (1995)	
	D1865	Davis et al., "A Means for Expressing Location Information in the Domain Name System," RFC 1876 (1996)	
	D1866	Cobb, "PPP Internet Protocol Extensions for Name Server Addresses," RFC 1877 (1995)	
	D1867	Thomson et al., "DNS Extensions to Support IP Version 6," RFC 1886 (1995)	
	D1868	Linn, "Generic Security Service Application Program Interface, Version 2," RFC 2078 (1997)	
	D1869	Vixie et al., "Dynamic Updates in the Domain Name System (DNS Update)," RFC 2136 (1997)	
	D1870	Eastlake, "Secure Domain Name System Dynamic Update," RFC 2137 (1997)	
	D1871	Rigney et al., "Remote Authentication Dial in User Service (Radius)," RFC 2138 (1997)	
	D1872	Rigney, "RADIUS Accounting," RFC 2139 (1997)	
	D1873	Allocchio, "Using the Internet DNS to Distribute Mixer Conformant Global Address Mapping," RFC 2163 (1998)	
	D1874	Daniel et al., "Resolution of Uniform Identifiers Using the Domain Name System," RFC 2168 (1997)	
	D1875	Elz et al., "Clarifications to the DNS Specification," RFC 2181 (1997)	
	D1876	Hamilton et al., "Use of DNS Aliases for Network Services," RFC 2219 (1997)	
	D1877	Kille et al., "Using Domains in LDAP/X.500 Distinguished Names," RFC 2247 (1998)	
	D1878	Bellovin et al., "Report of the IAB Security Architecture Workshop," RFC 2316 (1998)	
	D1879	Moats et al., "Building Directories from DNS: Experiences from WWWSeeker," RFC 2517 (1999)	
	D1880	Eastlake, "RSA/MD5 Keys and Sigs in the Domain Name System (DNS)," RFC 2537 (1999)	
	D1881	Eastlake, "Storage of Diffle-Hellman Keys in the Domain Name Systems (DNS)," RFC 2539 (1999)	
	D1882	Eastlake, "DNS Security Operational Considerations," RFC 2541 (1999)	
	D1883	Eastlake, "Reserved Top Level DNS Names," RFC 2606 (1999)	
	D1884	Aboba et al., "Proxy Chaining and Policy Implementation in Roaming," RFC 2607 (1999)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1885	Vixie, "Extensions Mechanisms for DNS (EDNSO)," RFC 2671 (1999)	
	D1886	Crawford, "Non-Terminal DNS Name Redirection," RFC 2672 (1999)	
	D1887	Srisuresh et al., "Security Model with Tunnel-Mode IPsec for NAT Domains," RFC 2709 (1999)	
	D1888	Eastlake, "Secret Key Establishment for DNS (TKEY RR)," RFC 2930 (2000)	
	D1889	Cisco Security Advisory: PIX Private Link Key Processing and Cryptography Issues (1998) available at http://www.cisco.com/warp/public/707/cisco-sa-19980603-pix-key.shtml	
	D1890	Gauntlet for IRIX Administrator's Guide (1985)	
	D1891	Gauntlet Firewall for UNIX; Administrator's Guide, Version 4.2 (1996-1998)	
	D1892	Gauntlet Firewall for UNIX; Getting Started Guide, Version 4.2 (1996-1998)	
	D1893	Gauntlet Firewall for UNIX; Netperm Table Reference Guide, Version 4.2 (1996-1998)	
	D1894	Gauntlet Firewall for UNIX, User Guide, Version 4.2 (1996-1998)	
	D1895	Snyder "Review: Firewalls," Network World (1998)	
	D1896	Schlaerth, "Service and Network Management Strategies for ATM in Wireless Networks," Bell Labs Technical Journal (2000)	
	D1897	Fischer et al., "Accounting Solutions in the UMTS Core Network," Bell Labs Technical Journal, 6(2):65-73 (2002)	
	D1898	Bakker et al., "Rapid Development and Delivery of Converged Services Using APLS," Bell Labs Technical Journal (2000)	
	D1899	La Roche et al., "High Speed Data Services Using the Switched Digital Broadband Access Systems," Bell Labs Technical Journal (1997)	
	D1900	Mooi Choo Chuah et al., "Mobile Virtual Private Dial-Up Services," Bell Labs Technical Journal (1999)	
	D1901	Fendick et al., "The PacketStar™ 6400 IP Switch – An IP Switch for the Converged Network," Bell Labs Technical Journal (1998)	
	D1902	Schulzrinne et al., "The Session Initiation Protocol: Providing Advanced Telephony Services Across the Internet," Bell Labs Technical Journal (1998)	
	D1903	Moganti et al., "A Framework for Understanding Network Intelligence," Bell Labs Technical Journal (2001)	
	D1904	Bosco et al., "Evolution of the Wide Area Network," Bell Labs Technical Journal (2000)	
	D1905	Raghavan et al., "Virtual Private Networks and Their Role in E-Business," Bell Labs Technical Journal, 6(2):99-115 (2002)	
	D1906	Sijben et al., "Application-Level Control of IP Networks: IP Beyond the Internet," Bell Labs Technical Journal (2001)	
	D1907	Kozik et al., "Voice Services in Next-Generation Networks: The Evolution of the Intelligent Network and its Role in Generating New Revenue Opportunities," Bell Labs Technical Journal (1998)	
	D1908	Brenner et al., "CyberCarrier Service and Network Management," Bell Labs Technical Journal (2000)	
	D1909	Stevens et al., "Policy-Based Management for IP Networks," Bell Labs Technical Journal (1999)	
	D1910	Milonas, "Enterprise Networking for the New Millennium," Bell Labs Technical Journal (2000)	
	D1911	Busschbach, "Toward QoS-Capable Virtual Private Networks," Bell Labs Technical Journal (1998)	
	D1912	McGee et al., "Dynamic Virtual Private Networks," Bell Labs Technical Journal, 6(2):116-135 (2002)	
	D1913	Veeraraghavan, "Connection Control in ATM Networks," Bell Labs Technical Journal (1997)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1914	Erfani et al., "Network Management: Emerging Trends and Challenges," Bell Labs Technical Journal (1999)	
	D1915	Rodriguez-Moral, "LIBRA-An Integrated Framework for Type of Service-Based Adaptive Routing in the Internet and Intranets," Bell Labs Technical Journal (1997)	
	D1916	Colbert et al., "Advanced Services: Changing How We Communicate," Bell Labs Technical Journal (2001)	
	D1917	Kocan et al., "Universal Premises Access to Voice Band and ATM Networks Using a Broadband Interworking Gateway," Bell Labs Technical Journal (1998)	
	D1918	Kozik et al., "On Opening PSTN to Enhances Voice/Data Services-The PINT Protocol Solution," Bell Labs Technical Journal (2000)	
	D1919	Doshi et al., "A Comparison of Next-Generation IP-Centric Transport Architectures," Bell Labs Technical Journal (1998)	
	D1920	Bergren et al., "Wireless and Wireline Convergence," Bell Labs Technical Journal (1997)	
	D1921	Al-Salameh et al., "Optical Networking," Bell Lab Technical Journal (1998)	
	D1922	Bauer, "IP Exchange Systems – Redefining Distributed Communications in the Enterprise," Bell Labs Technical Journal," (1999)	
	D1923	Dianda et al., "Reducing Complexity for Converged Voice/Data Networks and Services Architecture," Bell Labs Technical Journal (2000)	
	D1924	Meeuwissen et al., "The FRIENDS Platform-A Software Platform for Advanced Services and Applications," Bell Labs Technical Journal (2000)	
	D1925	Unmehopa et al., "The Support of Mobile Internet Applications in UMTS Networks Through the Open Service Access," Bell Labs Technical Journal 6(2):47-64 (2002)	
	D1926	Varadharajan et al., "Information Security and Privacy; Lecture Notes in Computer Science 1270," (1997)	
	D1927	Cisco Delivers Internet Infrastructure for Carrier-Class Voice Quality, April 28, 1998	
	D1928	Cisco Product Catalog, Cisco IP/VC 3500 Series – Videoconferencing Products, May 2000	
	D1929	Cisco Simplifies H.323 Multimedia Conferencing for Enterprises and Service Providers, April 28, 1998	
	D1930	Kotha, "Deploying H.323 Applications in Cisco Networks," White Paper, Cisco Systems, Inc. (1998)	
	D1931	H.332 Architecture and Design, Cisco Systems (2000)	
	D1932	Empowering The Internet Generation, Cisco Systems, Inc. (2000)	
	D1933	Intel and Cisco Complete Interoperability Tests to Deliver H.323 Connectivity, October 6, 1998	
	D1934	Spectrus Multipoint Video Conferencing Service Operational & Performance Specifications; Technical Reference Guide, Bellsouth, May 1995	
	D1935	Lambert, "IP Service Switches Could Give CLECs Hosted-App Portal Power," July 1, 1999 available at http://www.exhangmag.com/articles/971work1.html	
	D1936	IP Service Intelligence at the Edge; Enabling Value-Added Services Over DSL (April 2000)	
	D1937	Next Generation IP Conferencing Systems, Ridgeway Systems & Software; White Paper (1999)	
	D1938	Gupta et al., "Secure and Mobile Networking," Mobile Networks and Applications, 3:381-390 (1998)	
	D1939	Guin et al., "Application of Virtual Private Networking Technology to Standards-Based Management Protocols Across Heterogeneous Firewall-Protected Networks," IEEE (1999)	
	D1940	Zao et al., "A Public-Key Based Secure Mobile IP," Wireless Networks, J.C. Baltzer AG, Science Publishers, 5:373-390 (1999)	
	D1941	Wirbel, "Upgraded Tools Promse Scalable Virtual Networks," Electronic Engineering Times, pages 60 (1998)	
	D1942	Rescorla et al., "The Secure HyperText Transfer Protocol," RFC 2660 (1999)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1943	Lioy et al., "DNS Security," Terena Networking Conference, May 22-25, 2000	
	D1944	Gilmore et al., "Secure Remote Access to an Internal Web Server," IEEE Network (1999)	
	D1945	Kiuchi et al., "Using a WWW-based Mail User Agent for Secure Electronic Mail Service for Health Care Users," Methods of Information in Medicine, 37:247-253 (1998)	
	D1946	Kiuchi et al., "Automated Generation of a World Wide Web-Based Data Entry and Check Program for Medical Applications," Computer Methods and Programs in Biomedicine, 52:129-138 (1996)	
	D1947	Kiuchi et al., "A World Wide Web-Based User Interface for a Data Management System for Use in Multi-Institutional Clinical Trials – Development and Experimental Operation of an Automated Patient Registration and Random Allocation System," Elsevier Science Inc., 17:476-493 (1996)	
	D1948	Kiuchi et al., "University Medical Information Network – Past, Present, and Future," Medinfo (1998)	
	D1949	A Natural Extension of Cisco Systems IP Networking Expertise, The Cisco AS5300/Voice Gateway Relays High Quality Voice and Fax Traffic Across an IP Network, Data Sheet (1999)	
	D1950	Altiga Networks, Building Remote Access VPNs	
	D1951	VPN; The Remote Access Solution, A Comprehensive Guide to Evaluating: Security, Administration, Implementation (1997) available at www.compatible.com	
	D1952	10/100 Ethernet – DES I/O Card Administrator's Guide, Compatible Systems Corporation (1999) available at www.compatible.com	
	D1953	Compatiview 5.4 Reference Guide, Compatible Systems Corporation (1999) www.compatible.com	
	D1954	HSSI-DES I/O Card Administrator's Guide, Compatible Systems Corporation (1999) www.compatible.com	
	D1955	IntraPort 2 and IntraPort 2+ VPN Access Server Installation Guide, Compatible Systems Corporation (1998) www.compatible.com	
	D1956	IntraPortVPN Access Server Installation Guide, Compatible Systems Corporation (1998) www.compatible.com	
	D1957	IntraPort 2 and IntraPort 2+ VPN Access Server Administrator's Guide, Compatible Systems Corporation (1999) www.compatible.com	
	D1958	IntraPort Carrier-2 Chassis Administrator's Guide, Compatible Systems Corporation (1999) www.compatible.com	
	D1959	IntraPort Carrier-8 Chassis Administrator's Guide, Compatible Systems Corporation (1999) www.compatible.com	
	D1960	IntraPort Client Software Reference Guide, Compatible Systems Corporation (1999) www.compatible.com	
	D1961	IntraPort Enterprise-2 VPN Access Server; Administrator's Guide, Compatible Systems Corporation (1999) www.compatible.com	
	D1962	IntraPort Enterprise-8 VPN Access Server; Installation Guide, Compatible Systems Corporation (1999) www.compatible.com	
	D1963	Text-Based Configuration and Command Line Management; Reference Guide, Compatible Systems Corporation (1998) www.compatible.com	
	D1964	VPN Client Software Reference Guide, Compatible Systems Corporation (1999) www.compatible.com	
	D1965	Release Notes for Cisco Secure PIX Firewall Version 5.0(3), Cisco Systems (2000)	
	D1966	Valencia et al., "Cisco Layer Two Forwarding (Protocol) L2F," RFC 2341 (1998)	
	D1967	Schulzrinne, "SIP: Status and Directions," Department of Computer Science, Columbia University (1999)	
	D1968	Schulzrinne, "SIP: More Than Grandma's Phone Calls," Department of Computer Science, Columbia University (1999)	
	D1969	Willis, "The Future is SIP," ISSN: 1046-4468, 10(19):1046-4468 (1999)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** ***(Use as many sheets as necessary)***	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1970	Borthick, "Convergence Gets Complicated; Industry Trend or Event, ISSN:0162-3885, 29(11):6 (1999)	
	D1971	Vovida Networks and Nuera Communications Team to Enhance Vovida's Free SIP Protocol Stack for Voice over IP Applications; Business Wire (1999)	
	D1972	Kraskey et al., "NPN: Next-Generation Network Voice Services; Internet/Web/Online Service Information," ISSN:1093-8001 (1999)	
	D1973	Lucent Technologies Introduces the Elemedia™ SIP Server, A Software Platform for Integrated IP Telecommunications Services, PR Newswire Association, Inc. PR Newswire (1999)	
	D1974	3Com and Level 3 Test Next Generation of Telephone Systems and IP Networks to Speed the Deployment of New Business and Consumer Services, Business Wire, Inc. (2000)	
	D1975	Stahl, "Domain Administrators Guide," RFC 1032 (1987)	
	D1976	Partridge, "Mail Routing and the Domain System," RFC 974 (1986)	
	D1977	Mockapetris, "Domain System Changes and Observations," RFC 973 (1986)	
	D1978	Harrenstien et al., "DOD Internet Host Table Specification," RFC 952 (1985)	
	D1979	Postel, "Domain Name System Implementation Schedule – Revised," RFC 921 (1984)	
	D1980	Postel, Domain Name System Implementation Schedule – RFC 897 (1984)	
	D1981	Mockapetris, "Domain Name – Concepts and Facilities," RFC 882 (1983)	
	D1982	Postel, "The Domain Name Plan and Schedule," RFC 881 (1983)	
	D1983	Zaw-Sing Su, "The Domain Naming Convention for Internet User Applications," RFC 819 (1982)	
	D1984	Earrenstien et al., "Hostnames Server," RFC 811 (1982)	
	D1985	Postel, "Computer Mail Meeting Notes," RFC 805 (1982)	
	D1986	Luotonen, "Tunneling SSL Through a WWW Proxy," Internet-Draft (1997)	
	D1987	Luotonen, "Tunneling SSL Through a WWW Proxy," Internet-Draft (December 1995)	
	D1988	Luotonen, "Tunneling SSL Through a WWW Proxy," Internet-Draft (November 1995)	
	D1989	Luotonen, "Tunneling SSL Through a WWW Proxy," Internet-Draft (June 1995)	
	D1990	Cooper et al., "The US Domain," RFC 1386 (1992)	
	D1991	Rosenbaum, "Using the Domain Name System to Store Arbitrary String Attributes," Digital Equipment Corp., RFC 1464 (1993)	
	D1992	Cooper et al., "The US Domain," RFC 1480 (1993)	
	D1993	Gavron, "A Security Problem and Proposed Correction with Widely Deployed DNS Software," ACES Research Inc., RFC 1535 (1993)	
	D1994	Kumar et al, "Common DNS Implementation Errors and Suggested Fixes," RFC 1536 (1993)	
	D1995	Beertema, "Common DNS Data File Configuration Errors," RFC 1537 (1993)	
	D1996	Hanks et al., "Generic Routing Encapsulation over IPv4 Networks," RFC 1702 (1994)	
	D1997	Romao, "Tools for DNS Debugging," RFC 1713 (1994)	
	D1998	Eastlake et al., "Randomness Recommendations for Security," RFC 1750 (1994)	
	D1999	Federal Networking Council, "U.S. Government Internet Domain Names," RFC 1811 (1995)	
	D2000	Federal Networking Council, "U.S. Government Internet Domain Names," RFC 1816 (1995)	
	D2001	Karn et al., "The ESP DES-CBC Transform," RFC 1829 (1995)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2002	Hinden et al., "IP Version 6 Addressing Architecture," RFC 1884 (1995)	
	D2003	Schulzrinne et al., "RTP: A Transport Protocol for Real-Time Applications," Audio-Video Transport Working Group, RFC 1889 (1996)	
	D2004	Schulzrinne, "RTP Profile for Audio and Video Conferences with Minimal Control," RFC 1890 (1996)	
	D2005	Barr, "Common DNS Operational and Configuration Errors," RFC 1912 (1996)	
	D2006	Rekher et al., "Address Allocation for Private Internets," RFC 1918 (1996)	
	D2007	Deutsch, "ZLIB Compressed Data Format Specification Version 3.3," Network Working Group, RFC 1950 (1996)	
	D2008	Engebretson et al., "Registration in the MIL Domain," RFC 1956 (1996)	
	D2009	Elz et al., "Serial Number Arithmetic," RFC 1982 (1996)	
	D2010	Ohta, "Incremental Zone Transfer in DNS," RFC 1995 (1996)	
	D2011	Vixie, "A Mechanism for Prompt Notification of Zone Changes (DNS Notify)," Network Working Group, RFC 1996 (1996)	
	D2012	Manning et al., "Operational Criteria for Root Name Servers," Network Working Group, RFC 2010 (1996)	
	D2013	Speer et al., "RTP Payload Format of Sun's CellB Video Encoding," Network Working Group, RFC 2029 (1996)	
	D2014	Turletti et al., "RTP Payload Format for H.261 Video Streams," Network Working Group, RFC 2032 (1996)	
	D2015	Der-Danieliantz, "The AM (Armenia) Domain," Network Working Group, RFC 2053 (1996)	
	D2016	Rigney et al., "Remote Authentication Dial in User Service (Radius)," Network Working Group, RFC 2058 (1997)	
	D2017	Oehler et al., "HMAC-MDS IP Authentication with Replay Prevention," Network Working Group, RFC 2085 (1997)	
	D2018	Ashworth, "The Naming of Hosts," Network Working Group, RFC 2100 (1997)	
	D2019	Krawczyk et al., "HMAC: Keyed-Hashing for Message Authentication," Network Working Group, RFC 2104 (1997)	
	D2020	Bradner, "Key Words for Use in RFC s to Indicate Requirement Levels," Network Working Group, RFC 2119 (1997)	
	D2021	Crocker, "Mailbox Names for Common Services, Roles and Functions," Network Working Group, RFC 2142 (1997)	
	D2022	Federal Networking Council, "U.S. Government Internet Domain Names," Network Working Group, RFC 2146 (1997)	
	D2023	Elz et al., "Selection and Operation of Secondary DNS Service," Network Working Group, RFC 2182 (1997)	
	D2024	Zhu, "RTP Payload Format for H.263 Video Streams," Network Working Group, RFC 2190 (1997)	
	D2025	Perkins et al., "RTP Payload for Redundant Audio Data," Network Working Group, RFC 2198 (1997)	
	D2026	Cheng et al., "Test Cases for HMAC-MDS and HMAC-SHA-1," Network Working Group, RFC 2202 (1997)	
	D2027	Vaughan, "A Legal Basis for Domain Name Allocation," Network Working Group, RFC 2240 (1997)	
	D2028	Dierks et al., "The TLS Protocol Version 1.0," Network Working Group, RFC 2246 (1999)	
	D2029	Hoffman et al., "RTP Payload Format for MPEG1/MPEG2 Video," Network Working Group, RFC 2250 (1998)	
	D2030	Howard et al., "An Approach for Using LDAP as a Network Information Service," Network Working Group, RFC 2307 (1998)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2031	Andrews, "Negative Caching of DNS Queries (DNS NCACHE)," RFC 2308 (1998)	
	D2032	Eidnes et al., "Classless IN-ADDR.ARPA Delegation," Network Working Group, RFC 2317 (1998)	
	D2033	Schulzrinne et al., "Real Time Streaming Protocol (RTSP)," Network Working Group, RFC 2326 (1998)	
	D2034	Civanlar et al., "RTP Payload Format for Bundled MPEG," Network Working Group, RFC 2343 (1998)	
	D2035	Vaughan, "A Convention for Using Legal Names as Domain Names," Network Working Group, RFC 2352 (1998)	
	D2036	McDonald et al., "PF_Key Key Management API, Version 2," Network Working Group, RFC 2367 (1998)	
	D2037	Hinden et al., "IP Version 6 Addressing Architecture," Network Working Group, RFC 2373 (1998)	
	D2038	Hinden et al., "AN IPv6 Aggregatable Global Unicase Address Format," Network Working Group, RFC 2374 (1998)	
	D2039	Grimstad et al., "Naming Plan for Internet Directory-Enabled Applications," Network Working Group, RFC 2377 (1998)	
	D2040	Pereira, "IP Payload Compression Using DEFLATE," Network Working Group, RFC 2394 (1998)	
	D2041	Friend et al., "IP Payload Compression Using LZS," Network Working Group, RFC 2395 (1998)	
	D2042	Bormann et al., "RTP Payload Format for the 1998 Version of ITU-T Rec. H.263 Video (H.263+)," Network Working Group, RFC 2429 (1998)	
	D2043	Tynan, "RTP Payload Format for BT.656 Video Encoding," Network Working Group, RFC 2431 (1998)	
	D2044	Berc et al., "RTP Payload Format for JPEG-Compressed Video," Network Working Group, RFC 2435 (1998)	
	D2045	Pereira, "The ESP CBC-Mode Cipher Algorithms," Network Working Group, RFC 2451 (1998)	
	D2046	Casner et al., "Compressing IP/UDP/RTP Headers for Low-Speed Serial Links," Network Working Groups, RFC 2508 (1999)	
	D2047	Karn et al., "ICMP Security Failures Messages," Network Working Groups, RFC 2521 (1999)	
	D2048	Karn et al., "Photuris: Session-Key Management Protocol," Network Working Group, RFC 2522 (1999)	
	D2049	Eastlake, "DSA Keys and SIGs in the Domain Name System (DNS)," Network Working Group, RFC 2536 (1999)	
	D2050	Gilligan et al., "Basic Socket Interface Extensions for IPv6," Network Working Group, RFC 2553 (1999)	
	D2051	Newman, "Using TLS with IMAP, POP3 and ACAP," Network Working Group, RFC 2595 (1999)	
	D2052	Franks et al., "HTTP Authentication: Basic and Digest Access Authentication," Network Working Group, RFC 2617 (1999)	
	D2053	Hamzeh et al., "Point-to-Point Tunneling Protocol (PPTP)," Network Working Group, RFC 2637 (1999)	
	D2054	McKay, "RTP Payload Format for PureVoice™ Audio," Network Working Group, RFC 2658 (1999)	
	D2055	Rescorla, "The Secure HyperText Transfer Protocol," Network Working Group, RFC 2660 (1999)	
	D2056	Crawford, "Binary Labels in the Domain Name System," Network Working Group, RFC 2673 (1999)	
	D2057	Fox et al., "Virtual Private Networks Identifier," Network Working Group, RFC 2685 (1999)	
	D2058	Medvinskey, "Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)," Network Working Group, RFC 2712 (1999)	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2059	Rosenberg, et al., "An RTP Payload Format for Generic Forward Error Correction," Network Working Group, RFC 2733 (1999)	
	D2060	Fox et al., "NHRP Support for Virtual Private Networks," Network Working Group, RFC 2735 (1999)	
	D2061	Handley, et al., "Guidelines for Writers of RTP Payload Format Specifications," Network Working Group, RFC 2736 (1999)	
	D2062	Rosenberg et al., "Sampling of the Group Membership in RTP," Network Working Group, RFC 2762 (2000)	
	D2063	Gleeson et al., "A Framework for IP Based Virtual Private Networks," Network Working Group, RFC 2764 (2000)	
	D2064	Hellstrom, "RTP Payload for Text Conversation," Network Working Group, RFC 2793 (2000)	
	D2065	Aboba et al., "Implementation of L2TP Compulsory Tunneling via RADIUS," Network Working Group, RFC 2809 (2000)	
	D2066	Khare et al., "Upgrading to TLS within HTTP/1.1," Network Working Group, RFC 2817 (2000)	
	D2067	Rescorla, "HTTP Over TLS," Network Working Group, RFC 2818 (2000)	
	D2068	Daigle, "A Tangled Web: Issues of I18N, Domain Names, and the Other Internet Protocols," Network Working Group, RFC 2825 (2000)	
	D2069	Internet Architecture Board, "IAB Technical Comment on the Unique DNS Root," Network Working Group, RFC 2826 (2000)	
	D2070	Vixie et al., "Secret Key Transaction Authentication for DNS (TSIG)," Network Working Group, RFC 2845 (2000)	
	D2071	Petrack et al., "The PINT Service Protocol: Extensions to SIP and SDP for IP Access to Telephone Call Services," Network Working Group, RFC 2848 (2000)	
	D2072	Keromytis et al., "The Use of HMAC-RIPEMD-160-96 within ESP and AH," Network Working Group, RFC 2857 (2000)	
	D2073	Civanlar et al., "RTP Payload Format for Real-Time Pointers," Network Working Group, RFC 2862 (2000)	
	D2074	Rigney et al., "Remote Authentication Dial In User Service (RADIUS)," Network Working Group, RFC 2865 (2000)	
	D2075	Crawford et al., "DNS Extensions to Support IPv6 Address Aggregation and Renumbering," Network Working Group, RFC 2874 (2000)	
	D2076	Srisuresh, "Secure Remote Access with L2TP," Network Working Group, RFC 2888 (2000)	
	D2077	Mealling, "The Naming Authority Pointer (NAPTR) DNS Resource Record," Network Working Group, RFC 2915 (2000)	
	D2078	Muthukrishnan et al., "A Core MPLS IP VPN Architecture," Network Working Group, RFC 2917 (2000)	
	D2079	Chen, "Route Refresh Capability for BGP-4," Network Working Group, RFC 2918 (2000)	
	D2080	Eastlake et al., "Domain Name System (DNS) IANA Considerations," Network Working Group, RFC 2929 (2000)	
	D2081	Eastlake et al., DNS Request and Transaction Signatures," Network Working Group, RFC 2931 (2000)	
	D2082	Baugher et al., "Real-Time Transport Protocol Management Information Base," Network Working Group, RFC 2959 (2000)	
	D2083	Donovan, "The SIP INFO Method," Network Working Group, RFC 2976 (2000)	
	D2084	Wellington, "Secure Domain Name System (DNS) Dynamic Update," Network Working Group, RFC 3007 (2000)	
	D2085	Wellington, "Domain Name System Security (DNSSEC) Signing Authority," Network Working Group, RFC 3008 (2000)	
	D2086	Rosenberg et al., "Registration of parityfec MIME Types," Network Working Group, RFC 2000 (2000)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2087	Kikuchi et al., "RTP Payload Format for MPEG-4 Audio/Visual Streams," Network Working Group, RFC 3016 (2000)	
	D2088	Rosen et al., "Multiprotocol Label Switching Architecture," Network Working Group, RFC 3031 (2001)	
	D2089	Rosen et al., "MPLS Label Stack Encoding," Network Working Group, RFC 3032 (2001)	
	D2090	Anderson et al., "LDP Specification," Network Working Group, RFC 3036 (2001)	
	D2091	Thomas et al., "LDP Applicability," Network Working Group, RFC 3037 (2001)	
	D2092	Luthi, "RTP Payload Format for ITU-T Recommendation G.722.1," Network Working Group, RFC 2001 (2001)	
	D2093	Lennox et al., "Common Gateway Interface for SIP," Network Working Group, RFC 3050 (2001)	
	D2094	Heath et al., "IP Payload Compression Using ITU-T V.44 Packet Method," Network Working Group, RFC 3051 (2001)	
	D2095	Rawat et al., "Layer Two Tunneling Protocol (L2TP) over Frame Relay," Network Working Group, RFC 3070 (2001)	
	D2096	Klensin, "Reflections on the DNS, RFC 1591, and Categories of Domains," Network Working Group, RFC 3070 (2001)	
	D2097	Pall et al., "Microsoft Point-To-Point Encryption (MPPE) Protocol," Network Working Group, RFC 3078 (2001)	
	D2098	Zorn, "Deriving Keys for use with Microsoft Point-to-Point Encryption (MPPE)," Network Working Group, RFC 3079 (2001)	
	D2099	Campbell et al., "Control of Service Context Using SIP Request-URI," Network Working Group, RFC 3087 (2001)	
	D2100	Lewis, "DNS Security Extension Clarification on Zone Status," Network Working Group, RFC 3090 (2001)	
	D2101	Bremen et al., "Robust Header Compression (ROHC): Framework and Four Profiles: RTP, UDP,ESP, and Uncompressed," Network Working Group, RFC 3095 (2001)	
	D2102	Borella et al., "Realm Specific IP: Framework," Network Working Group, RFC 3102 (2001)	
	D2103	Borella et al., "Realm Specific IP: Protocol Specification," Network Working Group, RFC 3103 (2001)	
	D2104	Montenegro et al., "RSIP Support for End-to-End IPsec," Network Working Group, RFC 3104 (2001)	
	D2105	Eastlake, "RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)," Network Working Group, RFC 3110 (2001)	
	D2106	Finlayson, "A More Loss-Tolerant RTP Payload Format for MP3 Audio," Network Working Group, RFC 3119 (2001)	
	D2107	Thomas, "Requirements for Kerberized Internet Negotiation of Keys," Network Working Group, RFC 3129 (2001)	
	D2108	Lewis, "Notes from the State-of-the-Technology: DNSSEC," Network Working Group, RFC 3130 (2001)	
	D2109	Kempf, "Dormant Mode Host Alerting ("IP Paging") Problem Statement," Network Working Group, RFC 3132 (2001)	
	D2110	Verma et al., "L2TP Disconnect Cause Information," Network Working Group, RFC 3145 (2001)	
	D2111	Bush, "Delegation of IP6.ARPA," Network Working Group, RFC 3152 (2001)	
	D2112	Perkins et al., "RTP Testing Strategies," Network Working Group, RFC 3158 (2001)	
	D2113	Huston, "Management Guidelines & Operational Requirements for the Address and Routing Parameter Area Domain ("arpa")," Network Working Group, RFC 3172 (2001)	
	D2114	Shacham et al., "IP Payload Compression Protocol (IPComp)," Network Working Group, RFC 3173 (2001)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** ***(Use as many sheets as necessary)***	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2115	Kobayashi et al., "RTP Payload Format for DV (IEC 61834) Video," Network Working Group, RFC 3189 (2002)	
	D2116	Kobayashi et al., "RTP Payload Format for 12-bit DAT Audio and 20- and 24-bit Linear Sampled Audio," Network Working Group, RFC 3190 (2002)	
	D2117	Patel et al., "Securing L2TP Using IPsec," Network Working Group, RFC 3193 (2001)	
	D2118	Austein, "Applicability Statement for DNS MIB Extensions," Network Working Group, RFC 3197 (2001)	
	D2119	Hoffman, "SMTP Service Extensions for Secure SMTP over Transport Layer Security," Network Working Group, RFC 3207 (2002)	
	D2120	Conrad, "Indicating Resolver Support of DNSSEC," Network Working Group, RFC 3225 (2001)	
	D2121	Gudmundsson, "DNSSEC and IPv6 A6 Aware Server/Resolver Message Size Requirements," Network Working Group, RFC 3226 (2001)	
	D2122	Hardie, "Distributing Authoritative Name Servers via Shared Unicast Addresses," Network Working Group, RFC 3258 (2002)	
	D2123	Rosenberg et al., "SIP: Session Initiation Protocol," Network Working Group, RFC 3261 (2002)	
	D2124	Rosenberg et al., "Reliability of Provisional Responses in the Session Initiation Protocol (SIP)," Network Working Group, RFC 3262 (2002)	
	D2125	Resenberg et al., "Session Initiation Protocol (SIP): Locating SIP Servers," Network Working Group, RFC 3263 (2002)	
	D2126	Rosenberg et al., "An Offer/Answer Model with the Session Description Protocol (SDP)," Network Working Group, RFC 3264 (2002)	
	D2127	Roach et al., "Session Initiation Protocol (SIP)-Specific Event Notification," Network Working Group, RFC 3265 (2002)	
	D2128	Olson et al., "Support for IPv6 in Session Description Protocol (SDP)," Network Working Group, RFC 3266 (2002)	
	D2129	Sjoberg et al., "Real-Time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs," Network Working Group, RFC 3267 (2002)	
	D2130	Chown, "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)," Network Working Group, RFC 3268 (2002)	
	D2131	T'Jones et al., "Layer Two Tunneling Protocol (L2TP0:ATM Access Network Extensions," Network Working Group, RFC 3301 (2002)	
	D2132	Srisuresh et al., "Middlebox Communication Architecture and Framework," Network Working Group, RFC 3303 (2002)	
	D2133	Calhoun et al., "Layer Two Tunneling Protocol (L2TP) Differentiated Services Extension," Network Working Group, RFC 3308 (2002)	
	D2134	Niemi et al., "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)," Network Working Group, RFC 3310 (2002)	
	D2135	Rosenberg, "The Session Initiation Protocol (SIP) Update Method," Network Working Group, RFC 3311 (2002)	
	D2136	Camarillo et al., "Integration of Resource Management and SIP," Network Working Group, RFC 3312 (2002)	
	D2137	Marshall, "Private Session Initiation," Private Session Initiation Protocol (SIP) Extensions for Media Authorization," Network Working Group, RFC 3313 (2003)	
	D2138	Wasserman, "Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards," Network Working Group, RFC 3314 (2002)	
	D2139	Schulzrinne et al., "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers," Network Working Group, RFC 3319 (2003)	
	D2140	Price et al., "Signaling Compression (SigComp)," Network Working Group, RFC 3320 (2003)	
	D2141	Hannu et al., "Signaling Compression (SigComp) – Extended Operations," Network Working Group, RFC 3321 (2003)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2142	Hannu et al., "Signaling Compression (SigComp) Requirements & Assumptions," Network Working Group, RFC 3322 (2003)	
	D2143	Peterson, "A Privacy Mechanism for the Session Initiation Protocol," Network Working Group, RFC 3323 (2002)	
	D2144	Watson, "Short Term Requirements for Network Asserted Identity," Network Working Group, RFC 3324 (2002)	
	D2145	Jennings et al., "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks," Network Working Group, RFC 3325 (2002)	
	D2146	Schulzrinne et al., "The Reason Header Field for the Session Initiation Protocol (SIP)," Network Working Group, RFC 3326 (2002)	
	D2147	Willis et al., "Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contracts," Network Working Group, RFC 3327 (2002)	
	D2148	Arkko et al., "Security Mechanism Agreement for the Session Initiation Protocol (SIP)," Network Working Group, RFC 3329 (2003)	
	D2149	Charlton et al., "User Requirements for the Session Initiation Protocol (SIP) in Support of Deaf, Hard of Hearing and Speech-Impaired Individuals," Network Working Group, RFC 3351 (2002)	
	D2150	Singh et al., "Layer Two Tunneling Protocol (L2TP) Over ATM Adaptation Layer 5 (AAL5)," Network Working Group, RFC 3355 (2002)	
	D2151	Schulzrinne, "Dynamic Host Configuration Protocol (DHCP-for-Ipv4) Option for Session Initiation Protocol (SIP) Servers," Network Working Group, RFC 3361 (2002)	
	D2152	Bush et al., "Representing Internet Protocol Version 6 (IPv6) Addresses in the Domain Name System (DNS)," Network Working Group, RFC 3363 (2002)	
	D2153	Austein, "Tradeoffs in Domain Name System (DNS) Support for Internet Protocol Version 6 (IPv6)," Network Working Group, RFC 3364 (2002)	
	D2154	Caves et al., "Layer Two Tunneling Protocol "L2TP" Management Information Base," Network Working Group, RFC 3371 (2002)	
	D2155	Vemuri et al., "Session Initiation Protocol for Telephone (SIP-T): Context and Architectures," Network Working Group, RFC 3372 (2002)	
	D2156	Camarillo et al., "Grouping of Media Lines in the Session Description Protocol (SDP)," Network Working Group, RFC 338 (2002)	
	D2157	Zopf, "Real-Time Transport Protocol (RTP) Payload for Comfort Noise (CN)," Network Working Group, RFC 3389 (2002)	
	D2158	Camarillo et al., "Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping," Network Working Group, RFC 3398 (2002)	
	D2159	Mealling, "Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS," Network Working Group, RFC 3401 (2002)	
	D2160	Mealling, "Dynamic Delegation Discovery System (DDDS) Part Two: The Algorithm," Network Working Group, RFC 3402 (2002)	
	D2161	Mealling, "Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database," Network Working Group, RFC 3403 (2002)	
	D2162	Mealling, "Dynamic Delegation Discovery System (DDDS) Part Four: The Uniform Resource Identifiers (URI) Resolution Application," Network Working Group, RFC 3404 (2002)	
	D2163	Mealing, "Dynamic Delegation Discovery System (DDDS) Part Five: URI.ARPA Assignment Procedures," Network Working Group, RFC 3405 (2002)	
	D2164	Andersen, "Session Description Protocol (SDP) Simple Capability Declaration," Network Working Group, RFC 3407 (2002)	
	D2165	Sparks, "Internet Media Type Message/Sipfrag," Network Working Group, RFC 3420 (2002)	
	D2166	Lawrence, "Obsoleting Iquery," Network Working Group, RFC 3425 (2002)	
	D2167	Mankin et al., "Change Process for the Session Initiation Protocol (SIP)," Network Working Group, RFC 3427 (2002)	
	D2168	Campbell et al., "Session Initiation Protocol (SIP) Extension for Instant Messaging," Network Working Group, RFC 3428 (2002)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2169	Palter et al., "Layer-Two Tunneling Protocol Extension for PPP Link Control Protocol Negotiation," Network Working Group, RFC 3437 (2002)	
	D2170	Massay et al., "Limiting the Scope of the KEY Resource Record," Network Working Group, RFC 3445 (2002)	
	D2171	Garcia-Martin, "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)," Network Working Group, RFC 3455 (2003)	
	D2172	Patel et al., "Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPsec Tunnel Mode," Network Working Group, RFC 3456 (2003)	
	D2173	Kelly et al., "Requirements for IPsec Remote Access Scenarios," Network Working Group, RFC 3457 (2003)	
	D2174	Klensin, "Role of the Domain Name System (DNS)," Network Working Group, RFC 3467 (2003)	
	D2175	Garcia-Martin, "The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Static Dictionary for Signaling Compression (SigComp)," Network Working Group, RFC 3485 (2003)	
	D2176	Camarillo, "Compressing the Session Initiation Protocol (SIP)," Network Working Group, RFC 3486 (2003)	
	D2177	Schulzrinne, "Requirements for Resource Priority Mechanisms for the Session Initiation Protocol (SIP)," Network Working Group, RFC 3487 (2003)	
	D2178	Faltstrom et al., "Internationalizing Domain Names in Applications (IDNA)," Network Working Group, RFC 3490 (2003)	
	D2179	Hoffman et al., "Nameprep: A Stringprep Profile for Internationalized Domain Names (IDN)," Network Working Group, RFC 3491 (2003)	
	D2180	Costello, "Punycode: A Bootstring Encoding of Unicode for Internationalized Domain Names in Applications (IDNA)," Network Working Group, RFC 3492 (2003)	
	D2181	Gilligan et al., "Basic Socket interface Extensions for IPv6," Network Working Group, RFC 3493 (2003)	
	D2182	Gharai et al., "RTP Payload Format for Society of Motion Picture and Television Engineers (SMPTE) 292M Video," Network Working Group, RFC 3497 (2003)	
	D2183	Hinden et al., "Internet Protocol Version 6 (IPv6) Addressing Architecture," Network Working Group, RFC 3513 (2003)	
	D2184	Sparks, "The Session Initiation Protocol (SIP) Refer Method," Network Working Group, RFC 3515 (2003)	
	D2185	Camarillo et al., "Mapping of Media Streams to Resource Reservation Flows," Network Working Group, RFC 3524 (2003)	
	D2186	Kivinen et al., "More Modular Exponential (MODP) Diffie-Hellman Groups for Internet Key Exchange (IKE)," Network Working Group, RFC 3526 (2003)	
	D2187	Koren et al., "Enhanced Compressed RTP (CRTP) for Links with High Delay, Packet Loss and Reordering," Network Working Group, RFC 3545 (2003)	
	D2188	Blake-Wilson et al., "Transport Layer Security (TLS) Extensions," Network Working Group, RFC 3546 (2003)	
	D2189	Baugher et al., "The Group Domain of Interpretation," Network Working Group, RFC 3547 (2003)	
	D2190	Schulzrinne et al., "RTP: A Transport Protocol for Real-Time Applications," Network Working Group, RFC 3550 (2003)	
	D2191	Schulzrinne et al., "RTP Prole for Audio and Video Conferences with Minimal Control," Network Working Group, RFC 3551 (2003)	
	D2192	Bellovin et al., "On the Use of Stream Control Transmission Protocol (SCTP) with IPsec," Network Working Group, RFC 3554 (2003)	
	D2193	Casner et al., "MIME Type Registration of RTP Payload Formats," Network Working Group, RFC 3555 (2003)	
	D2194	Xie, "RTP Payload Format for European Telecommunications Standards Institute (ETSI) European Standard ES 201 108 Distributed Speech Recognition Encoding," Network Working Group, RFC 3557 (2003)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** ***(Use as many sheets as necessary)***	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2195	Li, "RTP Payload Format for Enhanced Variable Rate Codecs (EVRC) and Selectable Mode Vocoders (SMV)," Network Working Group, RFC 3558 (2003)	
	D2196	Press Release, Microsoft releases Windows NetMeeting 3 to the Web; New Version Now Available for Download (1999)	
	D2197	Microsoft Windows NetMeeting 3 Readme Windows 2000, Microsoft Corporation Business Review (1999)	
	D2198	Microsoft Windows NetMeeting 3.03 Beta 1 Readme, Microsoft Corporation (1999)	
	D2199	Baan Midmarket Solutions (BMS), Baan Can Company ,Microsoft Corporation Business Review (1998)	
	D2200	Portland Trail Blazers, Business Review, Microsoft Corporation Business Review (1998)	
	D2201	Deere & Company, Intranet Solutions, Microsoft Corporation Business Review (1997)	
	D2202	Dow Chemical, Microsoft Corporation Business Review (1998)	
	D2203	FileNet Corporation, Netmeeting, Microsoft Corporation Business Review (1997)	
	D2204	Ford Motor Company, Netmeeting, Microsoft Corporation Business Review (1997)	
	D2205	Irving, "Meet Me on the Internet," Internet Magazine Archive, Microsoft Corporation (1997)	
	D2206	Microsoft Netmeeting and the Role of Internet Conferencing for Deaf and Hard-of-Hearing Users, Netmeeting, Microsoft Corporation (1997)	
	D2207	Northrop Grumman, Microsoft Corporation Business Review (1998)	
	D2208	The Tompkins Group, Netmeeting, Microsoft Corporation Business Review (1997)	
	D2209	Toys "R" Us, Microsoft Business Review (1998)	
	D2210	Windows NetMeeting, Overview an Direction, Microsoft Corporation (1999)	
	D2211	PC Expo in New York, Technology for Business, Miller Freeman Group (1997-1999)	
	D2212	Microsoft Windows NetMeeting 3 Resource Kit, The Technical Guide to Installing, Configuring, and Supporting NetMeeting 3 in your Organization, Microsoft Corporation (1996-1999)	
	D2213	Hayes et al., Microsoft NetMeeting 3.0 Security Assessment and Configuration Guide, Systems and Network Attack Center, Version 1.14 (2001)	
	D2214	Schulzrinne, "The Session Initiation Protocol (SIP), Columbia University (1998-1999)	
	D2215	NetMeeting Data Conferencing Strategy, Microsoft Corporation (1998)	
	D2216	Integrating NetMeeting & TAPI 3.0, NetMeeting Development Team TAPI 3.0 IP Telephony Team, Microsoft Corporation (October 28, 1998)	
	D2217	Microsoft Windows NetMeeting 3 Resource Kit, The Technical Guide to Installing, Configuring, and Supporting NetMeeting 3 in your Organization, Microsoft Corporation (1996-2001)	
	D2218	ITU-T Recommendation T.127 "Terminals for Telematic Services –Multipoint Binary File Transfer Protocol," Telecommunication Standardization Sector of ITU (1995)	
	D2219	ITU-T Recommendation T.128 "Terminals for Telematic Services –Multipoint Application Sharing," Telecommunication Standardization Sector of ITU (1998)	
	D2220	ITU-T Recommendation T.140 "Series T: Terminal Equipment and Protocols for Telematic Services; Text Conversation Protocol for Multimedia Application," ITU-T – Telecommunication Standardization Sector of ITU (1997)	
	D2221	Buddy List: A Whitepaper, Microsoft Corporation (1997)	
	D2222	Corporate Remote Access Alternatives – iPass White Paper, November 21, 1998, iPass, Inc. ("IPASS")"	
	D2223	International Technical Support Organization, "Understanding OSF DCE 1.1 for AIX and OS/2," IBM (1995)	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2224	Wenger et al., "RTP Payload Format for H.264 Video," Network Working Group, RFC 3984 (2005)	
	D2225	Bryant et al., "Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture," Network Working Group, RFC 3985 (2005)	
	D2226	Berners-Lee, et al., "Uniform Resource Identifier (URI): Generic Syntax," Network Working Group, RFC 3986 (2005)	
	D2227	Duerst, et al., "International Resource Identifiers (IRIs)," Network Working Group, RFC 3987 (2005)	
	D2228	Schulzrinne, "Indication of Message Composition for Instant Messaging," Network Working Group, RFC 3994 (2005)	
	D2229	SonicWall/Aventail Whitepaper, SSL VPN Combined with Network Security. SonicWALL Clean VPN (2008)	
	D2230	Anyware Technology Announces Java Technology Security Product for Internet Communications, EverLink Suite Provides Secure Remote Network Access Via the Internet, (1998)	
	D2231	RSA Provides Security for Anyware Technology's Java-Based Internet Communications Product, EverLink Suite Incorporates RSA Technology to Provide Secure Remote Network Access, (1998)	
	D2232	Anyware Technology to Introduce New Channel Partner Program During Varvision 1998, Media Alert (1998)	
	D2233	Anyware Technology Launches Channel Partner Program, Company Builds VAR Channel for Its Everlink Suite of Secure Remote Access and Communications Software, News for Immediate Release (1998)	
	D2234	Anyware Technology Adds Three New Key Personnel, Fast Growing Software Developer Hires Director of Channel Sales, Telemarking Account Manager and Quality Assurance Engineer, News for Immediate Release (1998)	
	D2235	Anyware Technology Ships EverLink, The World's First Personal Virtual Private Network Software, News for Immediate Release (1998)	
	D2236	Anyware Technology Includes 30-Day Trial of Esafe Anti-Virus/Anti Vandal Software With Its Personal VPN Product, Pioneer of Remote Access & Secure Communications Software Partners with ESafe Technologies to Enhance EverLink Suite with Anti-Virus/Anti-Vandal Protection, News for Immediate Release (1998)	
	D2237	Anyware Technology Announces Strategic Var Partnerships with Codaram Corporation and RF Microsystems, Resellers Bring EverLink Suite of Secure Remote Access and Communications Software to Two Specific Vertical and Regional Markets, News for Immediate Release (1998)	
	D2238	Anyware Technology Ships New Version of Everlink Suite, Software Upgrade Brings New Levels of Flexibility and Ease of Use to Instant Secure Remote Access and Communications, News for Immediate Release (1999)	
	D2239	Quittek et al., "Definitions of Managed Objects for Robust Header Compression (ROHC)," Network Working Group, RFC 3816 (2004)	
	D2240	Townsley et al., "Layer 2 Tunneling Protocol (L2TP) Active Discovery Relay for PPP over Ethernet (PPPoE)," Network Working Group, RFC 3817 (2004)	
	D2241	Peterson et al., "Using E.164 Numbers with the Session Initiation Protocol (SIP)," Network Working Group, RFC 3824 (2004)	
	D2242	Polk et al., "Dynamic Host Configuration Protocol Option for Coordinate-Based Location Configuration Information," Network Working Group, RFC 3825 (2004)	
	D2243	Arkko et al., "MIKEY: Multimedia Internet KEYing," Network Working Group, RFC 3830 (2004)	
	D2244	Atkins et al., "Threat Analysis of the Domain Name System (DNS)," Network Working Group, RFC 3833 (2004)	
	D2245	Rosenberg et al., "Indicating User Agent Capabilities in the Session Initiation," Network Working Group, RFC 3840 (2004)	
	D2246	Rosenberg et al., "Caller Preferences for the Session Initiation Protocol (SIP)," Network Working Group, RFC 3841 (2004)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2247	Mahy, "A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)," Network Working Group, RFC 3842 (2004)	
	D2248	Schlyter, "DNS Security (DNSSEC) NextSECure (NSEC) RDATA Format," Network Working Group, RFC 3845 (2004)	
	D2249	Peterson, "S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)," Network Working Group, RFC 3853 (2004)	
	D2250	Rosenberg, "A Presence Event Package for the Session Initiation Protocol (SIP)," Network Working Group, RFC 3856 (2004)	
	D2251	Rosenberg, "A Watcher Information Event Template-Package for the Session Initiation Protocol (SIP), Network Working Group, RFC 3857 (2004)	
	D2252	Rosenberg, "An Extensible Markup Language (XML) Based Format for Watcher Information," Network Working Group, RFC 3858 (2004)	
	D2253	Peterson, "Common Profile for Presence (CPP)," Network Working Group, RFC 3859 (2004)	
	D2254	Peterson, "Common Profile for Instance Messaging (CPIM)," Network Working Group, RFC 3860 (2004)	
	D2255	Peterson, "Address Resolution for Instant Messaging and Presence," Network Working Group, RFC 3861 (2004)	
	D2256	Klyne et al, "Common Presence and Instant Messaging (CPIM): Message Format," Network Working Group, RFC 3862 (2004)	
	D2257	Sugano et al., "Presence Information Data Format (PIDF)," Network Working Group, RFC 3863 (2004)	
	D2258	Lennox et al., "Call Processing Language (CPL): A Language for User Control of Internet Telephony Services," Network Working Group, RFC 3880 (2004)	
	D2259	Touch et al., "Use of IPsec Transport Mode for Dynamic Routing," Network Working Group, RFC 3884 (2004)	
	D2260	Westerlund, "A Transport Independent Bandwidth Modifier for the Session Description Protocol (SDP)," Network Working Group, RFC 3890 (2004)	
	D2261	Mahy et al., "The Session Initiation Protocol (SIP) "Replaces" Header," Network Working Group, RFC 3891 (2004)	
	D2262	Sparks, "The Session Initiation Protocol (SIP) Referred-Vs. Mechanism," Network Working Group, RFC 3892 (2004)	
	D2263	Peterson, "Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) Format," Network Working Group, RFC 3892 (2004)	
	D2264	Durand et al., "DNS IPv6 Transport Operational Guidelines," Network Working Group, RFC 3901 (2004)	
	D2265	Niemi, "Session Initiation Protocol (SIP) Extension for Event State Publication," Network Working Group, RFC 3903 (2004)	
	D2266	Gurbani et al., "The Spirits (Services in PSTN Requesting Internet Services) Protocol," Network Working Group, RFC 3910 (2004)	
	D2267	Mahy et al., "The Session Initiation Protocol (SIP) "Join" Header," Network Working Group, RFC 3911 (2004)	
	D2268	Xiao et al., "Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)," Network Working Group, RFC 3916 (2004)	
	D2269	Lau et al., "Layer Two Tunneling Protocol – Version 3 (L2TPv3)," Network Working Group, RFC 3931 (2005)	
	D2270	Friend, "Transport Layer Security (TLS) Protocol Compression Using Lempel-Ziv-Stac (LZS)," Network Working Group, RFC 3943 (2004)	
	D2271	Kivinen et al., "Negotiation of NAT-Traversal in the IKE," Network Working Group, RFC 3947 (2005)	
	D2272	Huttunen et al., "UDP Encapsulation of IPsec ESP Packets," Network Working Group, RFC 3948 (2005)	
	D2273	Duric, "Real-Time Transport Protocol (RTP) Payload Format for Internet Low Bit Rate Codec (iLBC) Speech," Network Working Group, RFC 3952 (2004)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2274	Peterson, "Telephone Number Mapping (ENUM) Service Registration for Presence Services," Network Working Group, RFC 3953 (2005)	
	D2275	Daigle et al., "Domain-Based Applications Service Location Using SRV RRS and the Dynamic Delegation Discovery Service (DDDS)," Network Working Group, RFC 3958 (2005)	
	D2276	Camarillo, "The Early Session Disposition Type for the Session Initiation Protocol (SIP)," Network Working Group, RFC 3959 (2004)	
	D2277	Camarillo et al, "Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP), Network Working Group, RFC 3960 (2004)	
	D2278	Schulzrinne, "The tel URI for Telephone Numbers," Network Working Group, RFC 3966 (2004)	
	D2279	Camarillo, "The Internet Assigned Number Authority (IANA) Header Field Parameter Registry for the Session Initiation Protocol (SIP)," Network Working Group, RFC 3968 (2004)	
	D2280	Camarillo, "The Internet Assigned Number Authority (IANA) Uniform Resource Identifier (URI) Parameter Registry for the Session Initiation Protocol (SIP)," Network Working Group, RFC 3969 (2004)	
	D2281	Gurbani et al., "Interworking SIP and Intelligent Network (IN) Applications," Network Working Group, RFC 3976 (2005)	
	D2282	Frankel, et al, "The AES-XCBC-MAC-96 Algorithm and Its use with IPsec," Network Working Group, RFC 3556 (2003)	
	D2283	Goyret, "Signaling of Modem-On-Hold Status in Layer 2 Tunneling Protocol (L2TP)," Network Working Group, RFC 3573 (2003)	
	D2284	Soininen, "Transition Scenarios for 3GPP Networks," Network Working Group, RFC 3574 (2003)	
	D2285	Camarillo et al., "Mapping of Integrated Services Digital Network (ISDN) User Part (ISUP) Overlap Signaling to the Session Initiation Protocol (SIP)," Network Working Group, RFC 3578 (2003)	
	D2286	Rosenberg et al., "An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing," Network Working Group, RFC 3581 (2003)	
	D2287	Jason et al., "IPsec Configuration Policy Information Model," Network Working Group, RFC 3585 (2003)	
	D2288	Blaze et al., "IP Security Policy (IPSP) Requirements," Network Working Group, RFC 3586 (2003)	
	D2289	Thompson et al., "DNS Extensions to Support IP Version 6," Network Working Group, RFC 3596 (2003)	
	D2290	Gustafsson, "Handling of Unknown DNS Resource Record (RR) Types," Network Working Group, RFC 3597 (2003)	
	D2291	Frankel et al., "The AFS-CBC Cipher Algorithm and its use with IPsec," Network Working Group, RFC 3602 (2003)	
	D2292	Marshall et al., "Private Session Initiation Protocol (SIP) Proxy-to-Proxy Extensions for Supporting the PacketCable Distributed Call Signaling Architecture," Network Working Group, RFC 3603 (2003)	
	D2293	Huitema, "Real Time Control Protocol (RTCP) Attribute in Session Description Protocol," Network Working Group, RFC 3605 (2003)	
	D2294	Willis et al., "Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration," Network Working Group, RFC 3608 (2003)	
	D2295	Friedman et al., "RTP Control Protocol Extended Reports (RTCP XR)," Network Working Group, RFC 3611 (2003)	
	D2296	Van Der Meer et al., "RTP Payload Format for Transport of MPEG-4 Elementary Streams," Network Working Group, RFC 3640 (2003)	
	D2297	Kwan et al., "Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG)," Network Working Group, RFC 3645 (2003)	
	D2298	Droms, "DNS Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," Network Working Group, RFC 3646 (2003)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2299	Wellington et al., "Redefinition of DNS Authenticated Data (AD) Bit," Network Working Group, RFC 3655 (2003)	
	D2300	Gudmudsson, "Delegation Signer (DS) Resource Record (RR)," Network Working Group, RFC 3658 (2003)	
	D2301	Johnston et al., "Session Initiation Protocol (SIP) Basic Call Flow Examples," Network Working Group, RFC 3665 (2003)	
	D2302	Johnston et al., "Session Initiation Protocol (SIP) Public Switched Telephone Network (PSTN) Call Flows," Network Working Group, RFC 3666 (2003)	
	D2303	Rosenberg, "A Session Initiation Protocol (SIP) Event Package for Registrations," Network Working Group, RFC 3680 (2004)	
	D2304	Housley, "Using Advanced Encryption Standard (AES) Counter Mode with IPsec Encapsulating Security Payload (ESP)," Network Working Group, RFC 3686 (2004)	
	D2305	Cuellar et al., "Geopriv Requirements," Network Working Group, RFC 3693 (2004)	
	D2306	Danley et al., "Threat Analysis of the Geopriv Protocol," Network Working Group, RFC 3694 (2004)	
	D2307	Klensin, "Application Techniques for Checking and Transformation of Names," Network Working Group, RFC 3696 (2004)	
	D2308	Loughney et al., "Authentication, Authorization and Accounting Requirements for the Session Initiation Protocol (SIP)," Network Working Group, RFC 3702 (2004)	
	D2309	Huang et al., "A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers," Network Working Group, RFC 3706 (2004)	
	D2310	Baugher et al., "The Secure Real-Time Transport Protocol (SRTP)," Network Working Group, RFC 3711 (2004)	
	D2311	Aboba et al., "IPsec-Network Address Translation (NAT) Compatibility Requirements," Network Working Group, RFC 3715 (2004)	
	D2312	Aboba et al., "Securing Block Storage Protocols Over IP," Network Working Group, RFC 3723 (2004)	
	D2313	Rosenberg et al., "Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)," Network Working Group, RFC 3725 (2004)	
	D2314	Hollenbeck, "Transport Layer Security Protocol Compression Methods," Network Working Group, RFC 3749 (2004)	
	D2315	Nikander et al, "IPv6 Neighbor Discovery (ND) Trust Models and Threats," Network Working Group, RFC 3756 (2004)	
	D2316	Kolkman et al., "Domain in Name System Key (DNSKEY) Resource Record (RR) Secure Entry Point (SEP) Flag," Network Working Group, RFC 3757 (2004)	
	D2317	Faltstrom et al., "The E. 164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)," Network Working Group, RFC 3761 (2004)	
	D2318	Peterson, "Enumservice Registration for Session Initiation Protocol (SIP) Addresses of Record," Network Working Group, RFC 3764 (2004)	
	D2319	Arkko et al, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents," Network Working Group, RFC 3776 (2004)	
	D2320	Nagarajan, "Generic Requirements for Provider Provisioned Virtual Private Networks (PPVPN),"3809 (2004)	
	D2321	"Altiga Proves Multi-Vendor Interoperability for Seamless VPN Deployment; VPN Workshop Marks Significant Development in the VPN Market," Business Publications, Business Wire July 12, 1999	
	D2322	Thomas, "Recipe for E-Commerce,", IEEE Internet Computing, (1997) available for download at http://computer.org/internet/	
	D2323	Vyncke, "Build a Site to Site VPN Without Static Address," (1999)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** ***(Use as many sheets as necessary)***	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2324	Altiga Networks, Inc., Altiga VPN Concentrator Series (C50) Versus Nortel Networks Contivity Extranet Switch 4000 and 45000, VPN Tunneling Competitive Evaluation, The Tolly Group, (1999)	
	D2325	International Telecommunication Union; H.323, Series H: Audiovisual and Multimedia Systems; Infrastructure of Audiovisual Services – Systems and Terminal Equipment for Audiovisual Services (1999)	
	D2326	Cisco Systems, VPN 3000 Concentrator Series, User Guide; Release 2.5 (2000)	
	D2327	Cisco Systems, VPN 3000 Concentrator Series, Getting Started; Release 2.5 (2000)	
	D2328	Cisco Systems, VPN 3000 Client, User Guide; Release 2.5 (2000)	
	D2329	Cisco Simplifies H.323 Multimedia Conferencing for Enterprises and Service Providers, Multimedia Conference Manager Provides Policy Management for Voice over IP and Videoconferencing (1998) Article Available at http://web.archive.org/web/200006231265145/www.cisco.com/warp/public/146/pressroom/1998/apr98/25html	
	D2330	IP and Frame Relay: Bridging the Gap for Seamless and Secure Virtual Private Networking, White Paper, Cosine Communications (1998-2000)	
	D2331	Cisco Systems, Cisco IP/VC Quick Product Overview (1999)	
	D2332	Aziz et al., “Simple Key-Management for Internet Protocols,” IPSEC Working Group, Internet Draft (1996)	
	D2333	Karn et al., “Photuris: Session-Key Management Protocol,” Network Working Group, Internet Draft (1997)	
	D2334	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. the Automative Network eXchange (“ANX) references (1997, 1999)	
	D2335	Akamatsu et al., “Construction of Infrastructure for Global R&D,” Omron Technics, 38(3) Consecutive No. 127 (1998)	
	D2336	Zimmerer et al., “MIME Media Types for ISUP and QSIG Objects,” Network Working Group, Request for Comments: 3204 (2001)	
	D2337	Karn et al, “Photuris: Extended Schemes and Attributes,” Network Working Group, Request for Comments: 2523 (1999)	
	D2338	Klensin et al., “Domain Names and Company Name Retrieval,” Network Working Group, Request for Comments: 2345 (1998)	
	D2339	Gilligan et al., “Basic Socket Interface Extensions for IPv6,” Network Working Group, Request for Comments: 2133 (1997)	
	D2340	Libes, “Choosing a Name for Your Computer,” Network Working Group, Request for Comments: 1178 (1990)	
	D2341	Young, “New Protocol Connects Voice Over IP,” NetworkWorldFusion, Network World 12/13/1999	
	D2342	Mockapetris, “Domain Names – Implementation and Specification,” Network Working Group, Request for Comments: 883 (1983)	
	D2343	Handley, “Session Invitation Protocol,” Internet Engineering Task Force, Internet Draft (1996)	
	D2344	Berners-Lee, et al., “Uniform Resource Locators (URL),” Network Working Group, Request for Comments: 1738 (1994)	
	D2345	Response to RFP: Altiga, Network World Fusion, May 10, 1999	
	D2346	Agreement dated June 8, 1999 between Microsoft and Limelight Regarding Event Rental Charge.	
	D2347	Microsoft Netmeeting Conferencing Software, San Diego State University, Case Study Library (1999)	
	D2348	Networked Multimedia Technologies Enable Stanford Collaborative Learning Program, Stanford University: Creating a Virtual Master Builder Atelier, Draft: September 28, 1998	
	D2349	Compatible Systems Corporation; CompatiView 4 Reference Guide 1995-1997	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2350	Remote Access VPN User Authentication Model – VPN/VLAN Textbook, September 11, 1999." (English Abstract not Available)	
	D2351	Cisco PIX Firewall Series 1992-1999	
	D2352	IPR2014-00481; Inter Partes Review of Patent Number 7,188,180 filed on March 7, 2014, Petitioner Apple Inc., – Petition for Inter Partes Review, 65 pages	
	D2353	IPR2014-00481; Inter Partes Review of Patent Number 7.188.180 filed on March 7, 2014, Petitioner Apple Inc., – Exhibit 1029: Declaration of Michael Fratto Regarding U.S. Patent Number 7,188,180, 233 pages (2014)	
	D2354	IPR2014-00482; Inter Partes Review of Patent Number 7,188,180 filed on March 7, 2014, Petitioner Apple Inc., – Petition for Inter Partes Review, 68 pages	
	D2355	IPR2014-00482; Inter Partes Review of Patent Number 7.188.180 filed on March 7, 2014, Petitioner Apple Inc., – Exhibit 1029: Declaration of Michael Fratto Regarding U.S. Patent Number 7,188,180, 233 pages (2014)	
	D2356	IPR2014-00483; Inter Partes Review of Patent Number 7,987,274 filed on March 7, 2014, Petitioner Apple Inc., – Petition for Inter Partes Review, 63 pages	
	D2357	IPR2014-00483; Inter Partes Review of Patent Number 7,987,274 filed on March 7, 2014, Petitioner Apple Inc., – Exhibit 1029: Declaration of Michael Fratto Regarding U.S. Patent Number 7,188,180, 191 pages (2014)	
	D2358	IPR2014-00484; Inter Partes Review of Patent Number 7,987,274 filed on March 7, 2014, Petitioner Apple Inc., – Petition for Inter Partes Review, 63 pages	
	D2359	IPR2014-00484; Inter Partes Review of Patent Number 7,987,274 filed on March 7, 2014, Petitioner Apple Inc., – Exhibit 1029: Declaration of Michael Fratto Regarding U.S. Patent 7,987,274, 191 pages (2014)	
	D2360	IPR2014-00485; Inter Partes Review of Patent Number 8,051,181 filed on March 7, 2014, Petitioner Apple Inc., – Petition for Inter Partes Review, 73 pages	
	D2361	IPR2014-00485; Inter Partes Review of Patent Number 8,051,181 filed on March 7, 2014, Petitioner Apple Inc., – Exhibit 1011: Declaration of Dr. Roch Guerin, 24 pages (2014)	
	D2362	IPR2014-00485; Inter Partes Review of Patent Number 8,051,181 filed on March 7, 2014, Petitioner Apple Inc., – Exhibit 1029: Declaration of Michael Fratto, 448 pages (2014)	
	D2363	IPR2014-00485; Inter Partes Review of Patent Number 8,051,181 filed on March 7, 2014, Petitioner Apple Inc., – Exhibit 1014: US District Court Civil Docket 6:10cv94, Virnetx Inc. v. Microsoft Corporation dated August 21, 2013	
	D2364	IPR2014-00485; Inter Partes Review of Patent Number 8,051,181 filed on March 7, 2014, Petitioner Apple Inc., – Exhibit 1083: ITU-T Recommendation H.225.0; Call Signaling Protocols and Media Stream Packetization for Packet-Based Multimedia Communication Systems, Series H: Audiovisual and Multimedia Systems (1998)	
	D2365	IPR2014-00485; Inter Partes Review of Patent Number 8,051,181 filed on March 7, 2014, Petitioner Apple Inc., – Exhibit 1084: ITU-T Recommendation H.235; Security and Encryption for H-Series (H.323 and other H.245-Based) Multimedia Terminals, Series H: Audiovisual and Multimedia Systems (1998)	
	D2366	IPR2014-00485; Inter Partes Review of Patent Number 8,051,181 filed on March 7, 2014, Petitioner Apple Inc., – Exhibit 1085: ITU-T Recommendation H.245;Control Protocol for Multimedia Communication, Series H: Audiovisual and Multimedia Systems (1998)	
	D2367	IPR2014-00485; Inter Partes Review of Patent Number 8,051,181 filed on March 7, 2014, Petitioner Apple Inc., – Exhibit 1070: Joint Claim Construction and Prehearing Statement filed February 14, 2014	
	D2368	IPR2014-00485; Inter Partes Review of Patent Number 8,051,181 filed on March 7, 2014, Petitioner Apple Inc., – Exhibit 1071: Parties' Joint List of Proposed Construction of Remaining Disputed Claim Terms dated 2/25/2013	
	D2369	IPR2014-00486; Inter Partes Review of Patent Number 8,051,181 filed on March 7, 2014, Petitioner Apple Inc., – Petition for Inter Partes Review, 72 pages	
	D2370	IPR2014-00486; Inter Partes Review of Patent Number 8,051,181 filed on March 7, 2014, Petitioner Apple Inc., – Exhibit 1029: Declaration of Michael Fratto, 448 pages (2014)	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2371	Request for Inter Partes Reexamination of Patent Number 7,490,151 filed on August 16, 2011, Requester Cisco Systems., - Original Petition to Request Inter Partes Reexamination, 210 pages	
	D2372	BinTec Communications AG; Extended Feature Guide, Version 1.2 (1999)	
	D2373	Eagle Integrated Enterprise; Network Security System, 5.0 Reference Guide (1998)	
	D2374	Configuration Guide for the Cisco Secure PIX Firewall Version 5.0; Configuration Forms (1999)	
	D2375	Overview of Access VPNs and Tunneling Technologies, 1998, Cisco Systems, Inc.	
	D2376	Bianca/Brick-XMP; User's Guide – Hardware and Installation, Version 1.3 (1999)	
	D2377	Cisco Multimedia Conference Manager; Provides H.323 Gatekeeper and Proxy Services for Reliable and Scalable Videoconferencing and Voice-over-IP Deployments (1999)	
	D2378	Cisco Multimedia Conference Manager; Release 11.3 (Microsoft Invalidity Contentions Documents dated 3/20/14)	
	D2379	Trial Transcript in *VimetX Inc. v. Apple Inc.*, 6:10-cv-417 (E.D. Tex. Oct. 31, 2012 to Nov. 6, 2012)	
	D2380	VirnetX's Opening Claim Construction Brief, *VimetX Inc. v. Apple Inc.*, 6:11-cv-563, 6:12-cv-855 (E.D. Tex. Mar. 24, 2014)	
	D2381	IPR2014-00558; Inter Partes Review of Patent Number 6,502,135 filed on March 31, 2014, Petitioner Microsoft Corp., – Petition for Inter Partes Review, 56 pages	
	D2382	IPR2014-00558, Ex. 1003, Declaration of Dr. Roch Guerin submitted March 31, 2014 (41 pages)	

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.

Espacenet

Bibliographic data: GB2316841 (A) — 1998-03-04

Method for controlling a firewall

No documents available for this priority number.

Inventor(s): KUBOTA AYUMU; KATAGISHI KAZUKI; ASAMI TOHRU ± (AYUMU * KUBOTA, ; KAZUKI * KATAGISHI, ; TOHRU * ASAMI)

Applicant(s): KOKUSAI DENSHIN DENWA CO LTD [JP] ± (* KOKUSAI DENSHIN DENWA CO LTD)

Classification: - **international:** ***G06F13/00; H04L12/56; H04L12/66; H04L29/06;*** (IPC1-7): H04L9/32
- **cooperative:** **H04L29/06**; **H04L63/0263**; **H04L63/0272**; **H04L63/029**; H04W8/26; H04W80/04

Application number: GB19970018374 19970829

Priority number (s): JP19960227969 19960829

Also published as: GB2316841 (B) JPH1070576 (A) JP3662080 (B2)

Abstract of GB2316841 (A)

When a mobile terminal 21 connected to an Internet service provider (ISP) 30 intends to access an inner network 20 within a firewall 22 via the Internet 10, the ISP sends terminal user information to the inner network. An agent host 32 investigates the Internet protocol (IP) address and the account of the terminal and determines whether the mobile terminal is a terminal moved from the inner network based on this information. If this is the case, a host 23 managing the firewall sets a filter in the firewall allowing telecommunication between the mobile terminal and the inner network. The communication between the terminal and inner network may be by means of a two-way IP tunnel 40.

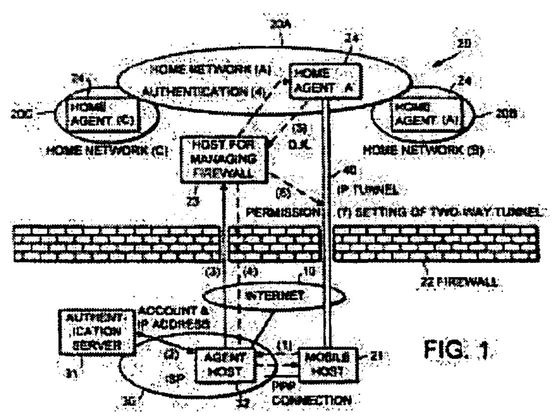


FIG. 1

Last updated: 11.12.2013 Worldwide Database 5.8.15; 93p

(12) UK Patent Application (19) GB (11) 2 316 841 (13) A

(43) Date of A Publication 04.03.1998

(21) Application No 9718374.3

(22) Date of Filing 29.08.1997

(30) Priority Data
(31) 08227969 (32) 29.08.1996 (33) JP

(71) Applicant(s)
Kokusai Denshin Denwa Co Ltd

(Incorporated in Japan)

3-2 Nishishinjuku 2-chome, Shinjuku-ku, Tokyo 163, Japan

(72) Inventor(s)
Ayumu Kubota
Kazuki Katagishi
Tohru Asami

(74) Agent and/or Address for Service
Boult Wade Tennant
27 Furnival Street, LONDON, EC4A 1PQ, United Kingdom

(51) INT CL[6]
H04L 9/32

(52) UK CL (Edition P)
H4P PPEB
H4L LDSC

(56) Documents Cited
INSPEC Abstract No.B9502-6210L-059, C9502-5620W-012 & Tenth Comp. Soc. Conference,1994,IEEE,pp212-18

(58) Field of Search
UK CL (Edition O) H4P PPEB
INT CL[6] H04L 9/32 12/22 29/06
Online:- WPI, INSPEC, JAPIO

(54) Method for controlling a firewall

(57) When a mobile terminal 21 connected to an Internet service provider (ISP) 30 intends to access an inner network 20 within a firewall 22 via the Internet 10, the ISP sends terminal user information to the inner network. An agent host 32 investigates the Internet protocol (IP) address and the account of the terminal and determines whether the mobile terminal is a terminal moved from the inner network based on this information. If this is the case, a host 23 managing the firewall sets a filter in the firewall allowing telecommunication between the mobile terminal and the inner network. The communication between the terminal and inner network may be by means of a two-way IP tunnel 40.

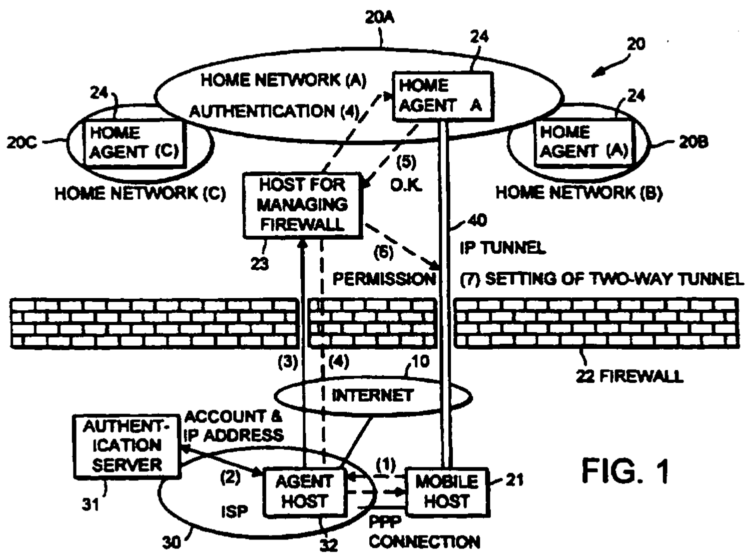


FIG. 1

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

GB 2 316 841 A

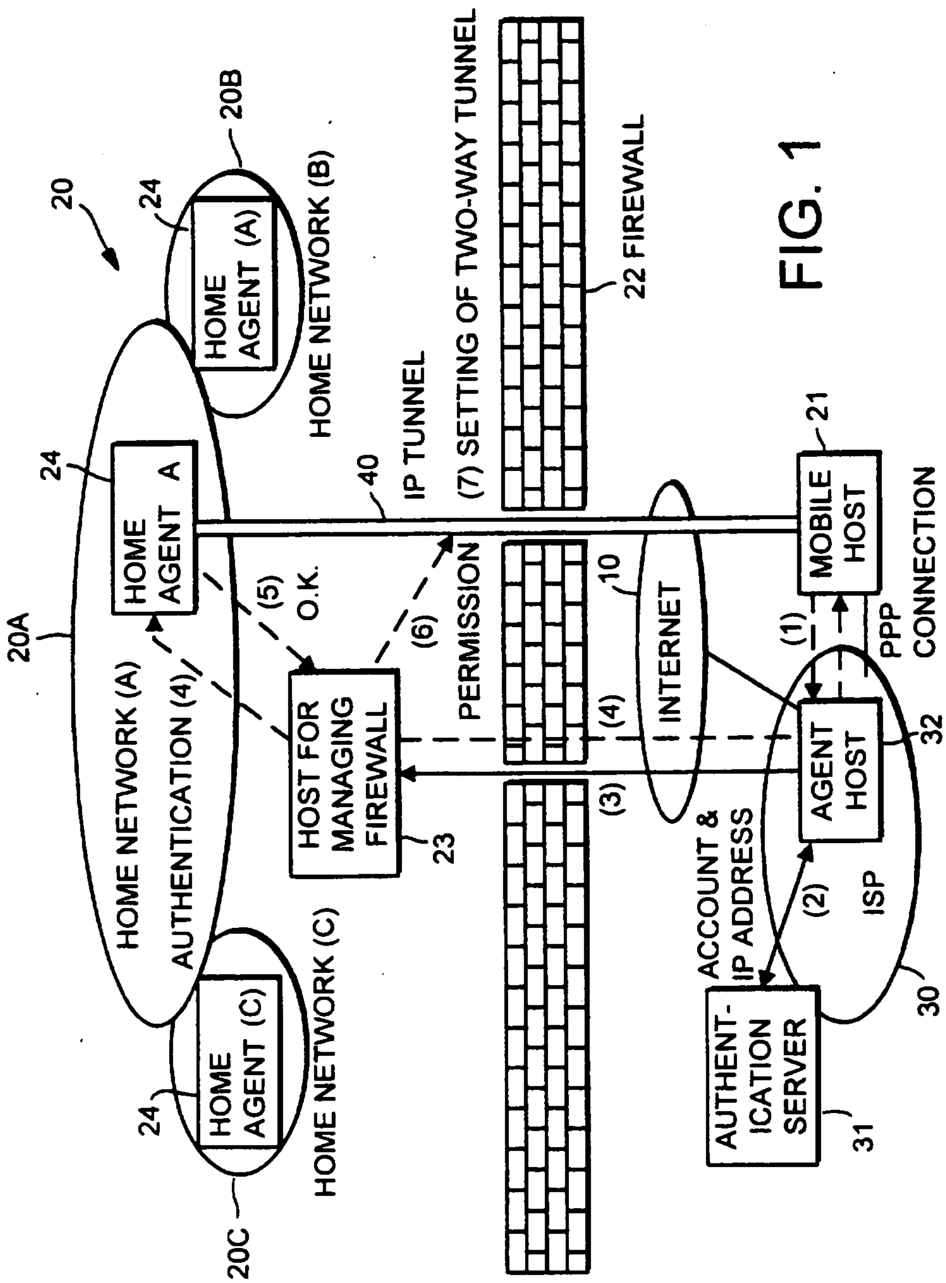

20
20A
20B
20C
24
HOME AGENT A
HOME AGENT (A)
HOME AGENT (C)
HOME NETWORK (A)
HOME NETWORK (B)
HOME NETWORK (C)
AUTHENTICATION (4)
(5) O.K.
(6) PERMISSION
HOST FOR MANAGING FIREWALL
23
40
IP TUNNEL
(7) SETTING OF TWO-WAY TUNNEL
22 FIREWALL
10
INTERNET
(3)
(4)
(1)
MOBILE HOST
21
PPP CONNECTION
AGENT HOST
32
ACCOUNT & IP ADDRESS
(2)
ISP
30
AUTHENT-ICATION SERVER
31

FIG. 1

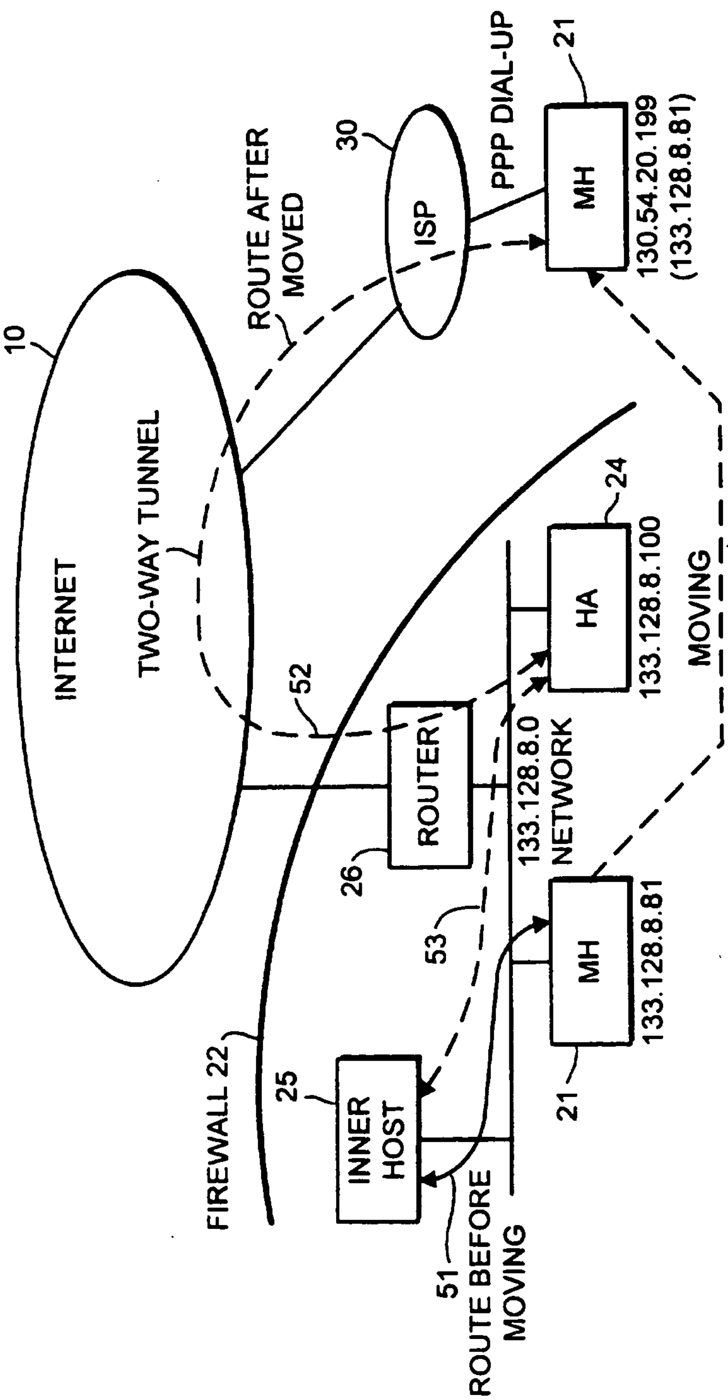


FIG. 2

MOBILE-IP (ADAPTIVE TO FIREWALL)

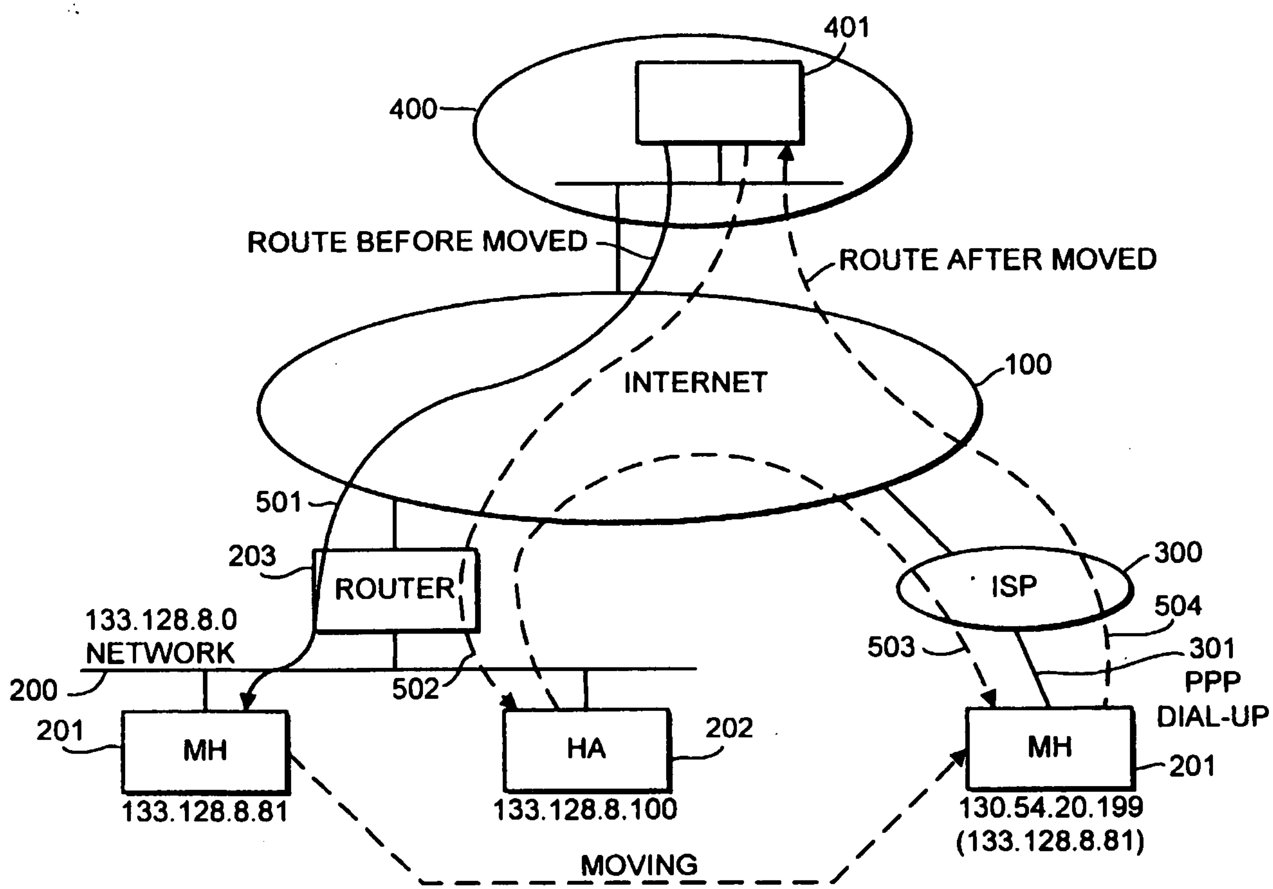


FIG. 3

PRIOR ART MOBILE-IP (NOT ADAPTIVE TO FIREWALL)

2316841

Specification

TITLE OF THE INVENTION

Method for dynamically controlling a firewall

FIELD OF THE INVENTION

This invention relates to a method for dynamically controlling a firewall.

BACKGROUND OF THE INVENTION

In a case of connecting a private network with the Internet, it is necessary to prevent a dishonest access from the Internet. However, if perfectly shut down a telecommunication between an internal network and an external network, it is impossible for a user of the internal network to access to his home network via the Internet.

Therefore, it is necessary to construct a firewall which selectively permits a telecommunication from an outside via the Internet.

In a prior art of a firewall, out of all data packets between the internal network and the external network, a previously permitted packet is only passed, but, another packet is shut down by using a filter.

Generally, such a filter is set by designating an IP (Internet Protokol) address of a terminal sending a packet, an IP address of a terminal receiving the packet, a kind of used protokol and a port number etc. For example, in a case of a telecommunication from an specific external IP address to any internal host (terminal) by using TCP (Transmission Control Protokol), a telecommunication using a specific port number (for example, 110) is permitted.

Wherein, the port number is an identifier for indicating a process of an upper layer in TCP or UDP (User Datagram Protokol).

However, it is difficult to obtain a pertinent filtering when a user accesses to his home network, by a dial-up or ppp connection via an ISP (Internet Service Provider) at outside of the home network, by using a mobile computer such as a note-type personal computer (a note-type PC), because upper 4 digits indicates a network with which the mobile PC is connected and lower 4 digits indicates an identifier of the mobile PC in the network, while the IP address used in the Internet telecommunication is indicated by 4 bytes number.

Namely, in a case of dial-up connection by a mobile host (MH) moved from its home network, the IP address assigned to the mobile host is different every connection, then it is impossible to take a telecommunication using an IP address assigned in its home network.

THerefore, it is difficult to set a filter in the firewall by designating an IP (Internet Protokol) address of the terminal sending a data packet and an IP address of the terminal receiving the data packet, because an IP address of a moved terminal is not constant in the dail-up connection.

Furthermore, it is not always possible for the user to use inner resources (a disk, data base and WWW etc.) of the home network to which he usually accesses, even if the filter of the firewall is pertinently set and it is possible only for an authorized mobile host and its user to permit an access from outside to the home network, because an access to the inner resources is individually limited and the access is permitted or is not permitted based on an IP address of a client terminal.

Next, referring to Fig.3, a mobile-IP address is explained, the mobile-IP is under work for standardization.

The mobile IP is a technique which enables to use a same IP address to the mobile terminal which moves anywhere, whenever the mobile terminal connects the Internet.

However, now, the mobile-IP is not adaptive to a network having the firewall.

In Fig.3, 100 denotes the Internet, 200 denotes a home network of a mobile terminal 201, 202 denotes a home agent (HA) on the home network 200, 203 denotes a router, 300 denotes an ISP, 400 denotes another network and 401 denotes a terminal on the network 400.

In Fig.3, an IP address of the home network 200 to which the mobile terminal 201 is usually connected is [133.128.8.0], an IP address of the mobile terminal 201 on the home network 200 is [133.128.8.81], an IP address of the home agent 202 is [133.128.8.100], and, an IP address of the mobile terminal 201 is [130.54.20.199] which is assigned by the ISP when the terminal 201 connects to the ISP by dial-up connection.

Generally, when a packet is sent from the terminal 401 on the network 400 to the terminal 201, as a rout 501 shown in Fig.3, the packet is transferred to the home network 200 to which the terminal 201 is usually connected. Therefore, when the terminal has been moved to another network, for example the ISP 300, it is necessary to transfer the packet to the network 300.

For transferring the packet, in the mobile-IP, an agent host is respectively provided to the network from which the mobile terminal is moved and the network to which the mobile terminal is moved. The agent in the network from which the mobile terminal is moved is called as a home agent and the agent in the network to which the mobile terminal is moved is called as a foreign agent. It is possible that the mobile terminal has a function of the foreign agent. In Fig.3, the mobile terminal 201 has a function of the foreign agent.

When the terminal 201 moved from its home network 200 connects to the ISP 300 by dial-up connection 301, a temporary IP address [130.54.2

0.199] is assigned to the terminal 201 by the ISP.

The IP address [130.54.20.199] of the mobile terminal 201 and its IP address [133.128.8.81] in the home network 200 are informed to the home agent 202 in the home network 200 via the ISP and the Internet100. Then, the home·agent 202 records that the terminal 201 having the IP [133. 128.8.81] is moving and its temporary IP address is [130.54.20.199] in its data base, based on the received information.

When a packet is sent from the terminal 401 in the network 400 to the terminal 201 by using the usual IP address [133.128.8.81], as shown by route 502, the home agent 202 receives the packet instead of the mobile terminal 201. Then, as shown by the route 503, the home agent 202 transfers the packet from the terminal 401 to the mobile terminal 201 via the Internet 100 and the ISP 300 to the mobile terminal 201, by embedding the packet from the terminal 401 into a packet forwarded to the temporary IP address [130.54.20.199]. The mobile terminal 201 obtains the original packet of the terminal 401 from the received packet, if necessary, as shown by the route 504, any packet to the terminal 401 via the ISP and the Internet.

As mentioned-above, in the mobile-IP, it is possible to a packet from the terminal 401 to the mobile terminal 201 by using the usual IP address [133.128.8.81].

However, the telecommunication using the temporary IP address [130. 54.20.199] is necessary between the mobile terminal 201 and the home agent 202.

Namely, in the mobile-IP, since any process is not applied to the packet send from the mobile terminal 201, an usual routing is necessary. Therefore, it is impossible for the mobile terminal 201 to another terminal inside the home network 200 except for the home agent 202 under the above-mentioned firewall, because only the telecommunication between the mobile terminal 201 and the home agent 202 is allowed. This means that the mobile terminal 201 is limited to access to the resource of its home network 200.

An object of the present invention is to provide a method for dynamically controlling a firewall which enables to set a filter pertinent to the mobile terminal being connected with the ISP (Internet Service Provider) by the dial-up connection and its user.

An object of embodiments of the present invention is to provide a method for dynamically controlling a firewall which enables to pertinently permit that said mobile terminal and its user access to the resource of the home network from outside.

The present invention enables to set a pertinent filter by obtaining a user information from an Internet service provider. Embodiments of the present invention resolve an limitation of an access to a resource of a home network by combining the filter setting with a mobile-IP.

According to the present invention there is provided a method for enabling a pertinent filter comprising the steps of:

a step for sending a user information of a terminal being connected to an internet service provider by dial-up connection to an inner network inside a firewall from said internet service provider when said terminal accesses to said inner network via the Internet.

a step that said inner network determines whether said terminal is a mobile terminal moved from said inner network, based on said user information;

a step for setting a filter of said firewall to permit a telecommunication between said terminal when said terminal is said mobile terminal moved from said inner network.

In a method embodying the present invention, for resolving an limitation of an access, further an

IP tunnel is used after setting of said filter for a telecommunication between said terminal and inner network.

In another embodiment for resolving an limitation of an access, said user information is transferred between an agent host provided in said internet service provider and a host for managing said firewall which sets said filter of said firewall provided in said inner network, and said telecommunication using said IP tunnel is done between said terminal and a home agent provided in said inner network.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 shows a configuration of a system to which a method embodying the present invention is applied.

Fig. 2 shows a mobile-IP which is adaptive to a firewall.

Fig. 3 shows an prior art mobile-IP which is not adaptive to a firewall.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

An embodiment of the present invention will be explained referring to the drawings.

In Fig. 1, 10 denotes the Internet, 20 denotes an inner network having plural home networks 20A, 20B and 20C, 21 denotes a mobile terminal which is usually connected to the inner network 20, 22 denotes a firewall, 23 denotes a host for managing the firewall, 24 denotes a home agent provided in each of home networks 20A, 20B and 20C, 30 denotes an ISP (Internet Service Provider), 31 denotes a server for authentication in the ISP, 32 denotes an agent host in the ISP.

The mobile terminal 21 has a function of a foreign agent for mobile-IP. The mobile terminal 21 is intended to connect the inner network 20 via the Internet, by dial-up connection to the ISP at any location after moving from the home network.

In this embodiment, a mechanism for controlling the firewall based on a user information obtained from the ISP and a mobile-IP mechanism adaptive to the firewall are provided.

The mechanism for controlling the firewall 22 based on the user information obtained from ISP 30 will be explained referring to Fig.1.

A user account (ID) and a pass word are input to the ISP 30, when a user of the mobile terminal 21 intends to connect to the ISP 30 by the dial-up connection. In the ISP 30, the authentication server 31 determines whether the user input data are proper or not. Only when the user input data are proper, an IP address is assigned to the mobile terminal 21, then the mobile terminal 21 is connected to the Internet 100. For this purpose, the ISP 30 can always grasp which user is connecting to the ISP 30 based on the user information and which IP address is assigned to the mobile terminal 21.

When the inner network 20 can know the user and an IP address used by the user, by obtaining the user information from the ISP 30, it is possible to properly set the filter. Then, it is possible to permit a telecommunication from a user who is previously allowed to access to the inner network 20 and to exclude an access from a user who has not authority for the access.

In Fig.1, a mechanism for adding and/or deleting a filter is provided, by providing the host 23 for managing the firewall within the inner network 20. Further, the agent host 32 is provided within the ISP so that only the telecommunication between the agent host 32 and the host 23 for managing the firewall can be allowed. Since the hosts 23 and 32 can use a fixed IP address for this telecommunication, there is no problem on setting the filter for the firewall.

Concretely, the filter is set by the following steps (1)~(7). The step (n) corresponds to an symbol (n) in Fig,1.

(1) When the mobile terminal 21 intends to access to the inner network

20 from outside of it, the mobile terminal 21 requests an establishment of the connection between the mobile terminal 21 and the inner network 20 via the the agent host 32 in the ISP.

(2) The agent host 32 investigates an IP address and an account at dial-up connection of the mobile terminal 21.

(3) The agent host 32 relays a message from the mobile terminal 21 to the host 23 for managing the firewall, only when the mobile terminal 21 is connected by using a specific account which is allowed to access inside the firewall 22.

(4) An authentication is done by end-to-end method between the mobile terminal 21 and the home agent 24 via the host 23 for managing the firewall, because, in mobile-IP, an authentication must be done between the mobile terminal and the home agent.

(5) If the authentication is successful, the home agent sends a message of the success to the host 23 for managing the firewall.

(6) Then, the host 23 for managing the firewall changes the setting of the firewall 22 so as to permit the telecommunication between the mobile terminal 21 and the home agent 24.

(7) At the time when the host 23 for managing the firewall enables the telecommunication between the mobile terminal 21 and the home agent 24 by changing the setting of the firewall 22, the host 23 informs it to the home agent 24 and the host 23 informs it to the mobile terminal 21 via the agent host 32. After receiving the message, the home agent 24 sets an IP tunnel to the mobile terminal 21 and the mobile terminal 21 sets an IP tunnel to the home agent 24, then a two-way IP tunnel 40 is set.

By using the two-way IP tunnel 40, the mobile terminal 21 telecommunicates with each terminal of the inner network 20. Wherein, the mobile terminal 21 periodically sends a message for maintaining the connection to the host 23 for managing the firewall. When the message for maintaining the connection from a certain mobile terminal stops, the host 23 for managing the firewall automatically deletes the filter setting to the mobile terminal.

As mentioned above, it is possible to set the firewall 22 only within a necessary term and only for the telecommunication of which start point and end point are distinctly restricted.

A specification of the mobile-IP which is under work for standardization is not adaptive to the network 20 having the firewall 22.

Then, the mobile-IP is improved to adapt to the firewall 22 as follows, and the improved mobile-IP is combined with the above-mentioned filter setting.

An combination of the mobile-IP and the dynamic firewall control will be explained referring to Fig.2.

As a route 52 shown in Fig.2, a packet from the mobile terminal 21 to the terminal 25 inside the firewall 22 is embedded in a packet to the home agent 24, then sent out. The home agent 24 obtains an original packet out of the received packet. The home agent 24 sends the obtained packet to the inner terminal 25, as a route 53 shown in Fig.2, by sends again the obtained packet to the Internet. In Fig.2, 26 denotes a router. When the mobile terminal exist in the inner network 20, the mobile terminal 21 telecommunicates with the inner terminal 25 via a route 51.

As mentioned-above, even if an authority is individually allowed in the inner network 20, it is possible to permit the access based on the IP address of the mobile terminal 21 which is usually connected with the network 20 by using the two-way tunnel between the mobile terminal 21 and the home agent 24. Therefore, it is possible to communicate between the mobile terminal 21 and the inner terminal 25.

According to the present invention, it is possible to set the firewall so as to permit the communication from the specific user in connection with the ISP by dail-up connection.

Further, according to embodiments of the present invention, because of an improvement and an combination of the mobile-IP, it is possible to access to the resources of the inner network from outside as same as connected with the inner network.

WHAT IS CLAIMED IS:

1. A method for dynamically controlling a firewall comprising steps of:

a step for sending a user information of a terminal being connected to an internet service provider by dial-up connection to an inner network inside a firewall from said internet service provider when said terminal accesses to said inner network via the Internet;

a step that said inner network determines whether said terminal is a mobile terminal moved from said inner network, based on said user information;

a step for setting a filter of said firewall to permit a telecommunication between said terminal when said terminal is said mobile terminal moved from said inner network.

2. The method claimed in claim 1 wherein, an IP tunnel is used after setting of said filter for a telecommunication between said terminal and said inner network.

3. The method claimed in claim 2 wherein, said user information is transferred between an agent host provided in said internet service provider and a host for managing said firewall which sets said filter of said firewall provided in said inner network, and said telecommunication using said IP tunnel is done between said terminal and a home agent provided in said inner network.

4. A method for dynamically controlling a firewall substantially as hereinbefore described with reference to the accompanying drawings.

The Patent Office

12

Application No:	GB 9718374.3	**Examiner:**	Matthew Nelson
Claims searched:	1-4	**Date of search:**	20 November 1997

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.O): H4P (PPEB)

Int Cl (Ed.6): H04L 9/32, 12/22, 29/06

Other: Online:- WPI, JAPIO, INSPEC

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
X	INSPEC Abstract No. B9502-6210L-059, C9502-5620W-012 & "Tenth Annual Computer Security Applications Conference", published 1994, IEEE, pp212-18, Goldberg "The MITRE security perimeter" (see abstract).	

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.
		E	Patent document published on or after, but with priority date earlier than, the filing date of this application.
&	Member of the same patent family		

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **09-266475**
(43)Date of publication of application : **07.10.1997**

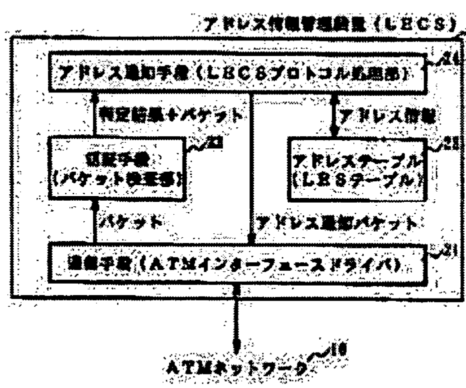
(51)Int.Cl. H04L 12/22
G06F 15/00
G09C 1/00
G09C 1/00
H04L 9/32

(21)Application number : **08-073601**
(22)Date of filing : **28.03.1996**

(71)Applicant : **HITACHI LTD**
(72)Inventor : **SAWADA SUNAO**
SUGAWARA MASAKATSU
NISHIKAWA JIKAI

(54) **ADDRESS INFORMATION MANAGEMENT EQUIPMENT AND NETWORK SYSTEM**

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent an illicit user from acquiring a correct address by reporting other wrong address to be camouflaged as a normal address to the illicit user.



SOLUTION: Upon the receipt of a packet requesting an address of an LES, an ATM interface driver 21 gives the packet to packet check section 22. The packet check section 22 checks the content of the packet and discriminates it to be valid when the content is in matching with a preset range or to be an illicit request when not and reports the result of discrimination to a LECS protocol processing section 24 with the packet. When the result of discrimination indicates a valid packet, the LECS protocol processing section 24 retrieves an LES table 23 and generates an address notice packet including the LES address and reports the packet to a request source via the ATM interface driver 21. When the discrimination results indicates an illicit request, the processing section 24 reports an address notice packet including an address for hacker countermeasure terminal equipment to the request source via the driver 21.

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－266475

(43)公開日　平成９年(1997)10月７日

(51)Int.Cl.⁶	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ 12/22		9466－5K	Ｈ０４Ｌ 11/26	
Ｇ０６Ｆ 15/00	３３０		Ｇ０６Ｆ 15/00	３３０Ａ
Ｇ０９Ｃ 1/00	６４０	7259－5Ｊ	Ｇ０９Ｃ 1/00	６４０Ｚ
	６６０	7259－5Ｊ		６６０Ｅ
Ｈ０４Ｌ 9/32			Ｈ０４Ｌ 9/00	６７１

審査請求　未請求　請求項の数４　ＯＬ　（全 ５ 頁）

(21)出願番号　特願平8－73601

(22)出願日　平成８年(1996) ３月28日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　澤田　素直
神奈川県川崎市幸区鹿島田890番地の12株式会社日立製作所情報・通信開発本部内

(72)発明者　菅原　征勝
神奈川県横浜市戸塚区戸塚町5030番地株式会社日立製作所ソフトウェア開発本部内

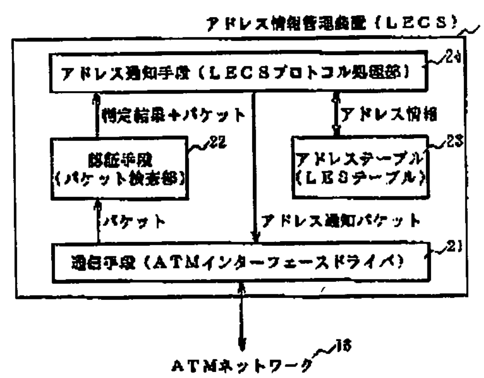
(72)発明者　西川　慈海
神奈川県横浜市戸塚区戸塚町5030番地株式会社日立製作所ソフトウェア開発本部内

(74)代理人　弁理士　小川　勝男

(54)【発明の名称】　アドレス情報管理装置およびネットワークシステム

(57)【要約】
【課題】不正な要求元に対してアドレス情報の通知を拒否したことを知られることなく正しいアドレス情報を渡すことを防ぎ，不正なアクセスの記録を取ることを可能にするアドレス情報管理方法を提供する。
【解決手段】アドレス情報管理装置１は通信手段２１，認証手段２２，アドレステーブル２３，アドレス通知手段２４より構成される。

図２



PATENT ABSTRACTS OF JAPAN

(11)Publication number : **10-032610**
(43)Date of publication of application : **03.02.1998**

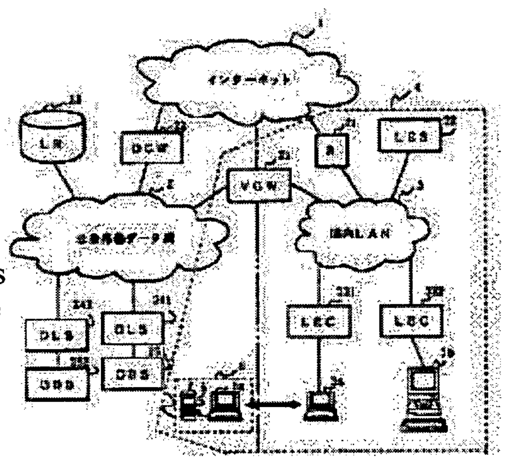
(51)Int.Cl. H04L 12/66
H04L 12/46
H04L 12/28

(21)Application number : **08-203015**
(22)Date of filing : **12.07.1996**

(71)Applicant : **NEC CORP**
(72)Inventor : **TOMOIKE HIROMOTO**

(54) VIRTUAL PRIVATE NETWORK CONSTITUTING METHOD IN MOBILE DATA COMMUNICATION

(57)Abstract:
PROBLEM TO BE SOLVED: To execute a data communication by one IP address by connecting a public mobile data network constituting a virtual private network with private branch LAN through a gate way so as to convert data to a mobile terminal to an address.
SOLUTION: When a data terminal 3a connected to the subordinate of the LAN emulation server 32 of private branch LAN 3 stops connection with a LAN switch 331 and connects with a mobile equipment 5, the call control part of the mobile equipment 5 is informed of the address of the data terminal 3a. The mobile terminal 5 houses the informed address in a memory to form a mobile data terminal 6 accessable to the public mobile data network 2 and receives the kind of service, the number of the virtual private network and the node number from a location register 23. The server 32 retrieves address information of the terminal 3a and converts data to the mobile terminal 5 to an address to execute data communication by one IP address.



(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平10－32610

(43)公開日　平成10年(1998) 2月3日

(51)Int.Cl.⁶		識別記号	庁内整理番号	ＦＩ			技術表示箇所
ＨＯ４Ｌ	12/66		9744－5K	ＨＯ４Ｌ	11/20	Ｂ	
	12/46				11/00	３１０Ｃ	
	12/28					３１０Ｂ	

審査請求　有　　請求項の数５　ＦＤ　（全 14 頁）

(21)出願番号　特願平8－203015

(22)出願日　平成8年(1996) 7月12日

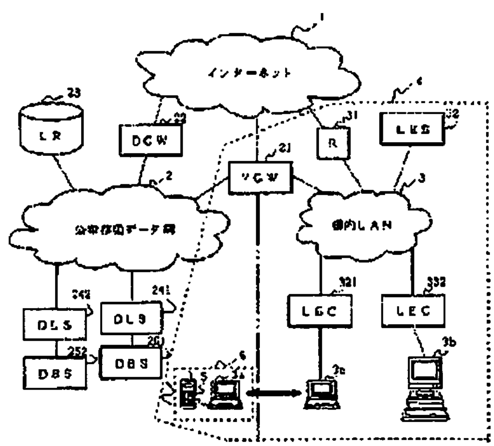
(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　友池　裕元
東京都港区芝五丁目７番１号　日本電気株式会社内

(74)代理人　弁理士　加藤　朝道

(54)【発明の名称】　移動データ通信における仮想私設網の構成方法

(57)【要約】
【課題】インターネット接続を許容する移動データ通信網を利用した仮想私設網を構築する際に問題となる、ＩＰルーティングの問題を無くし、構内ＬＡＮ端末が公衆移動データ網へアクセスしている移動環境においても構内ＬＡＮに接続されている端末と自由に通信可能となるような仮想私設網サービスの提供。
【解決手段】ＬＡＮエミュレーションサーバを有する構内ＬＡＮと公衆移動データ網とをＬＡＮエミュレーションクライアント機能を有する仮想私設網ゲートウェイを介して接続し、該ゲートウェイは、ＩＰアドレスと公衆移動データ網内アドレスとの変換機能を備える。公衆移動データ網は移動データ端末からの位置登録要求受信時に該移動データ端末が属するゲートウェイに該移動データ端末が移動した旨通知する機能を備える。



PATENT ABSTRACTS OF JAPAN

(11)Publication number : **11-355271**
(43)Date of publication of application : **24.12.1999**

(51)Int.Cl. H04L 12/22
H04L 12/56

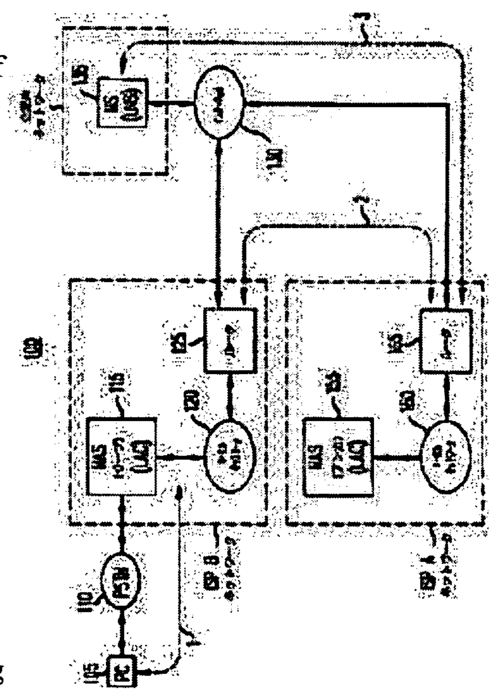
(21)Application number : **11-126562**
(22)Date of filing : **07.05.1999**

(71)Applicant : **LUCENT TECHNOL INC**
(72)Inventor : **CHUAH MOOI CHOO**
RAI GIRISH

(30)Priority
Priority number : **98 74582** Priority date : **08.05.1998** Priority country : **US**

(54) MOBILE POINT-TO-POINT PROTOCOL

(57)Abstract:
PROBLEM TO BE SOLVED: To incorporate a hand-off function of transferring an existing PPP connection from one network access server(NAS) to another NAS by establishing a call through a tunnel to a first packet server connected to a user in response to a call request message, transmitting a disconnection message and disconnecting the tunnel used before.
SOLUTION: When providing a virtual private network service for an employee at a distant place to perform access through a network server(NS) 135 to the network of a company by an internet service provider(ISP) A, for example, the remote user is sometimes located at a section to become the object of the service of an ISP B temporarily. At such a time, in response to the call request message, a serve LAC 115 establishes the call through the tunnel to an anchor LAC 155 connected to the user. Then, the disconnection message is transmitted and the tunnel used before is disconnected for supporting a call from the user.



(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－355271

(43)公開日　平成11年(1999)12月24日

(51)Int.Cl.⁶　識別記号　ＦＩ
ＨＯ４Ｌ　12/22　　ＨＯ４Ｌ　11/26
　12/56　　11/20　１０２Ａ

審査請求　未請求　請求項の数15　ＯＬ　（全 19 頁）

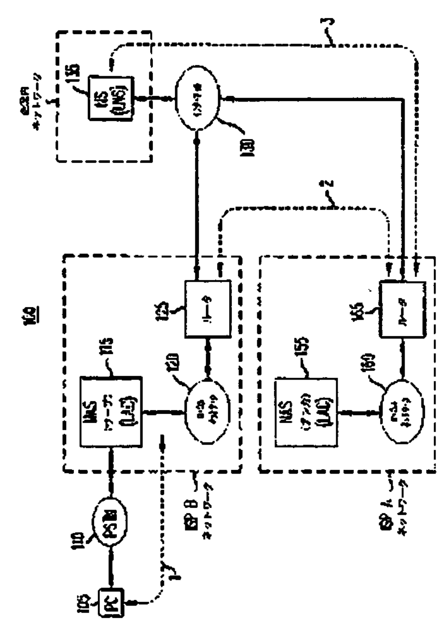
(21)出願番号　特願平11－126562
(22)出願日　平成11年(1999)5月7日
(31)優先権主張番号　０９／０７４５８２
(32)優先日　1998年5月8日
(33)優先権主張国　米国（ＵＳ）

(71)出願人　596092698
ルーセント　テクノロジーズ　インコーポレーテッド
アメリカ合衆国，07974－0636　ニュージャーシィ，マレイ　ヒル，マウンテン　アヴェニュー　600
(72)発明者　ムーイ　チョー　チュー
アメリカ合衆国　07724　ニュージャーシィ，イートンタウン，イートンクレスト　ドライヴ　148ビー
(74)代理人　弁理士　岡部　正夫　（外11名）

最終頁に続く

(54)【発明の名称】　移動ポイント・ツー・ポイント・プロトコル

(57)【要約】
【課題】　本発明は、通信におけるパケット通信システムに関し、特に無線環境における仮想私設網(Vertual Private Network)に関する技術を提供する。
【解決手段】　本発明は、呼要求メッセージに応動して、ユーザに接続された第１のパケット・サーバへトンネルを介して呼を確立し、そして、切断メッセージを他のパケット・サーバに送信して、該ユーザからの該呼をサポートするために以前使用されていたトンネルを切断する、パケット・サーバからなることを特徴とする。これにより、ネットワークアクセスサーバが既存のＰＰＰ接続を１つのＮＡＳから別のＮＡＳに移転できる「ハンドオフ」機能がネットワーク・アクセス・サーバに組み込まれる。



PATENT ABSTRACTS OF JAPAN

(11)Publication number : **10-070576**
(43)Date of publication of application : **10.03.1998**

---

(51)Int.Cl.

H04L 12/66
G06F 13/00
G06F 13/00
H04L 12/24
H04L 12/26

---

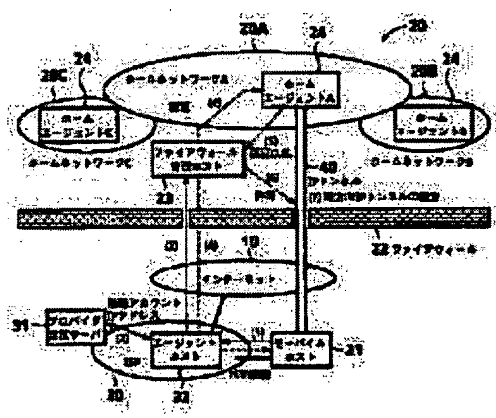
(21)Application number : **08-227969**
(22)Date of filing : **29.08.1996**

(71)Applicant : **KOKUSAI DENSHIN DENWA CO LTD <KDD>**
(72)Inventor : **KUBOTA AYUMI**
KATAGISHI KAZUOKI
ASAMI TORU

---

(54) **FIRE WALL DYNAMIC CONTROL METHOD**

(57)Abstract:
PROBLEM TO BE SOLVED: To properly execute the filter setting of a fire wall to a moving terminal dial-up-connected to an internet service provider(ISP) and its user and to properly permit access to a home network resource.
SOLUTION: When the terminal 21 dial-up-connected to ISP 30 access to an internal network 20 within the fire wall 22 through the internet 10, user information of the terminal 21 is sent from ISP 30 to judge whether the terminal 21 is a moving terminal moved from the internal network 20 based on this user information. When it is the moving terminal, the filter of the fire wall 22 is set to permit communication between the terminal 21 and the internal network 20, and communication between the terminal 21 and the internal network 20 is executes through an IP tunnel.



(19)日本国特許庁（JP）　(12) 公開特許公報(A)　(11)特許出願公開番号

特開平10－70576

(43)公開日　平成10年(1998)3月10日

(51)Int.Cl.⁶		識別記号	庁内整理番号	F I			技術表示箇所
H04L	12/66		9744－5K	H04L	11/20	B	
G06F	13/00	353		G06F	13/00	353T	
		357				357Z	
H04L	12/24		9744－5K	H04L	11/08		
	12/26						

審査請求　未請求　請求項の数3　OL　（全 7 頁）

(21)出願番号　特願平8－227969

(22)出願日　平成8年(1996)8月29日

(71)出願人　000001214
国際電信電話株式会社
東京都新宿区西新宿2丁目3番2号

(72)発明者　稲田　歩
東京都新宿区西新宿二丁目3番2号　国際電信電話株式会社内

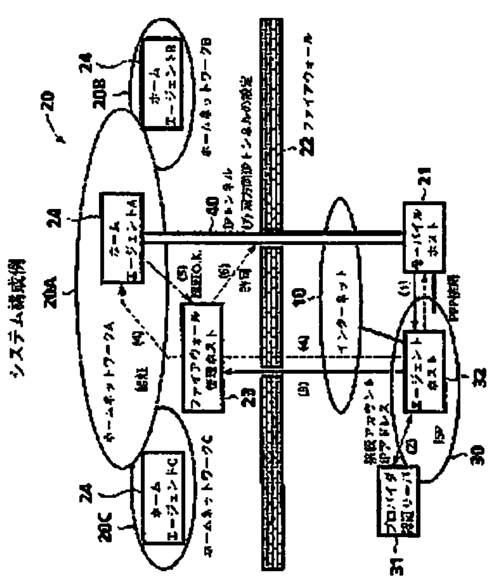
(72)発明者　片岸　一起
東京都新宿区西新宿二丁目3番2号　国際電信電話株式会社内

(72)発明者　浅見　徹
東京都新宿区西新宿二丁目3番2号　国際電信電話株式会社内

(74)代理人　弁理士　光石　俊郎　（外2名）

(54)【発明の名称】　ファイアウォール動的制御方法

(57)【要約】
【課題】　インターネットサービスプロバイダ（ISP）にダイヤルアップ接続中の移動端末及びそのユーザに対してファイアウォールのフィルタ設定を適切に行い、更に、ホームネットワーク資源へのアクセスを適切に許可できること。
【解決手段】　ISP30にダイアルアップにより接続中の端末21がインターネット10を経由してファイアウォール22内の内部ネットワーク20にアクセスする際に、ISP30から端末21のユーザ情報を送り、このユーザ情報を基に端末21が内部ネットワーク20から移動した移動端末であるか否かを判断し、移動端末である場合に、同端末21と内部ネットワーク20との通信を許可するようにファイアウォール22のフィルタを設定し、更に、同端末21と内部ネットワーク20との通信をIPトンネル40により行う。



PATENT ABSTRACTS OF JAPAN

(11)Publication number : **11-261704**
(43)Date of publication of application : **24.09.1999**

(51)Int.Cl.

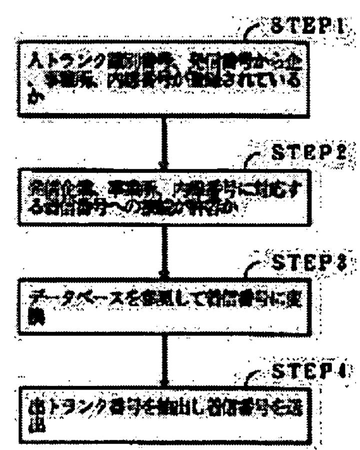
H04M 3/42
H04L 12/46
H04L 12/28
H04L 12/66
H04M 3/00
H04Q 3/545
H04Q 3/58

(21)Application number : **10-061200**
(22)Date of filing : **12.03.1998**

(71)Applicant : **FUJITSU LTD**
(72)Inventor : **WAKIMOTO TAKESHI**
OHASHI MASAHIKO

(54) CONNECTION METHOD FOR VIRTUAL NETWORK AND GATEWAY EXCHANGE

(57)Abstract:
PROBLEM TO BE SOLVED: To realize a connection method connected by means of the function of a gateway exchange without revising a numbering plan in the case of connecting prescribed business offices in plural private networks by a virtual network connected by the gateway exchanges as of the connection method and the gateway exchanges in the virtual network where the prescribed business offices in the plural private networks are connected by the gateway exchanges.
SOLUTION: This gateway exchange discriminates whether or not an enterprise, an office and an extension number of a caller are registered in a virtual network from an incoming trunk identification number and a caller number of a call (STEP1), discriminates whether or not the connection to an incoming call number is allowed to correspond to the enterprise, the office and the extension number of the caller (STEP2), converts the incoming call number into an incoming call number in a private network by referencing a database when the



connection to the incoming call number is allowed (STEP3) and acquires an outgoing trunk and sends the incoming call number thereto (STEP4).

(19)日本国特許庁（JP）　(12)公開特許公報(A)　(11)特許出願公開番号

特開平11－261704

(43)公開日 平成11年(1999)9月24日

(51)Int.Cl.6	識別記号	FI		
H04M 3/42		H04M	3/42	E
H04L 12/46			3/00	B
12/28		H04Q	3/545	
12/66			3/58	106
H04M 3/00		H04L	11/00	310C

審査請求 未請求 請求項の数3 OL (全11頁) 最終頁に続く

(21)出願番号 特願平10－61200

(22)出願日 平成10年(1998)3月12日

(71)出願人 000005223
富士通株式会社
神奈川県川崎市中原区上小田中4丁目1番1号

(72)発明者 脇本 武志
愛知県名古屋市東区東桜一丁目13番3号
富士通名古屋通信システム株式会社内

(72)発明者 大橋 正彦
愛知県名古屋市東区東桜一丁目13番3号
富士通名古屋通信システム株式会社内

(74)代理人 弁理士 井桁 貞一

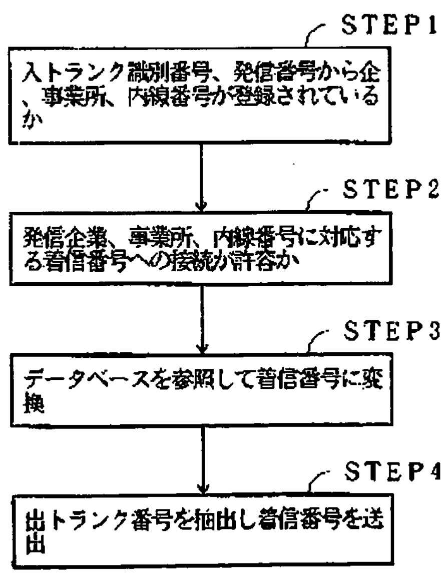
(54)【発明の名称】仮想ネットワークの接続方法およびゲートウェイ交換機

(57)【要約】

【課題】本発明は、複数の私設網の所定の事業所をゲートウェイ交換機で接続した仮想ネットワークにおける接続方法、およびゲートウェイ交換機に関し、複数の私設網の所定の事業所をゲートウェイ交換機で接続した仮想ネットワークで接続を行うとき、番号計画の変更を行うことなく、ゲートウェイ交換機の機能で接続する接続方法を実現することを目的とする。

【解決手段】ステップ1でゲートウェイ交換機は発呼してきた入トランク識別番号、発信番号から、発信者の企業、事業所、内線番号が仮想ネットワークに登録されているかを判定し、ステップ2で発信者の企業、事業所、内線番号対応に着信番号への接続が許容されているかを判定し、ステップ3で着信番号への接続が許容の場合、着信番号をデータベースと参照して、私設網の着信番号に変換し、ステップ4で出トランクを捕捉して着信番号を送出するように構成する。

本発明の第1の原理を説明する図



PATENT ABSTRACTS OF JAPAN

(11)Publication number : **10-126440**

(43)Date of publication of application : **15.05.1998**

(51)Int.Cl. H04L 12/56
G06F 13/00
H04L 12/46
H04L 12/28
H04L 12/24
H04L 12/26
H04L 29/06

(21)Application number : **08-275809**

(22)Date of filing : **18.10.1996**

(71)Applicant : **HITACHI LTD**

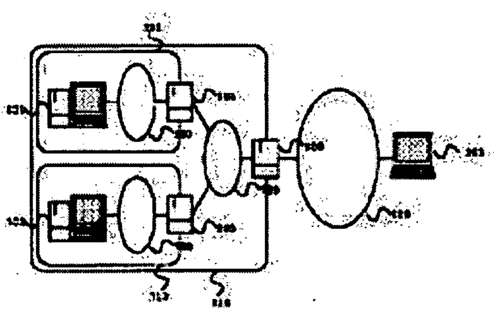
(72)Inventor : **KAYASHIMA MAKOTO**
TERADA MASATOSHI
FUJIYAMA TATSUYA
OGINO TAKAAKI

(54) NETWORK COMMUNICATION METHOD AND EQUIPMENT

(57)Abstract:

PROBLEM TO BE SOLVED: To obtain a virtual network environment in which communication is attained without notifying a relay path in the network communication system where communication between a client and a server is conducted in an environment in which a plurality of fire walls are interposed.

SOLUTION: A communication relay program that relays a communication client program on a client 303 and a communication server program of servers 301, 302 is started on servers 304, 305, 306 such as a fire wall, a relay path control table is provided to the client 303 and the relay servers 304-306, the communication client program is connected to the relay program of the relay server communicated by the client selected from the table in the connection processing to a server whose direct connection is unable due to a fire wall to request the relay of communication with the communication server program on the server to the relay server.



(19)日本国特許庁（ＪＰ）　　(12) 公開特許公報(A)　　(11)特許出願公開番号

特開平10－126440

(43)公開日　平成10年(1998)5月15日

(51)Int.Cl.⁶		識別記号	FI		
H04L	12/56		H04L	11/20	102D
G06F	13/00	355	G06F	13/00	355
H04L	12/46		H04L	11/00	310C
	12/28			11/08	
	12/24			13/00	305B

審査請求　未請求　請求項の数22　ＯＬ　（全 13 頁）　最終頁に続く

(21)出願番号　特願平8－275309

(22)出願日　平成8年(1996)10月18日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目6番地

(72)発明者　萱島　信
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内

(72)発明者　寺田　真敏
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内

(72)発明者　藤山　達也
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　小川　勝男

最終頁に続く

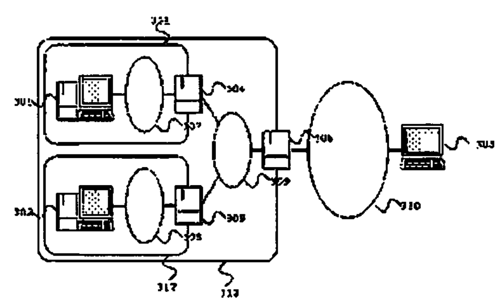
(54)【発明の名称】　ネットワーク通信方法および装置

(57)【要約】　　（修正有）

【課題】複数のファイアウォールが介在する環境でクライアントとサーバとの通信を行なうネットワーク通信システムにおいて，中継経路を意識せずに通信できる仮想ネットワーク環境を得る。

【解決手段】クライアント３０３上の通信クライアントプログラムと，サーバ３０１，３０２の通信サーバプログラムの通信を中継する通信中継プログラムをファイアウォール等中継サーバ３０４，３０５，３０６上で起動し，クライアントおよび中継サーバには中継経路制御テーブルを持たせ，通信クライアントプログラムは，ファイアウォールにより直接接続できないサーバへの接続処理において、前記テーブルより選択したクライアントから通信可能な中継サーバの中継プログラムに接続し、通信サーバプログラムとの通信の中継を依頼する。更に、サーバへの接続処理において、クライアントの通信クライアントプログラムと同様に、中継サーバにサーバ上の通信サーバプログラムとの通信の中継を依頼する。

図3



PATENT ABSTRACTS OF JAPAN

(11)Publication number : . **11-355272**
(43)Date of publication of application : **24.12.1999**

(51)Int.Cl. H04L 12/22
H04L 12/56

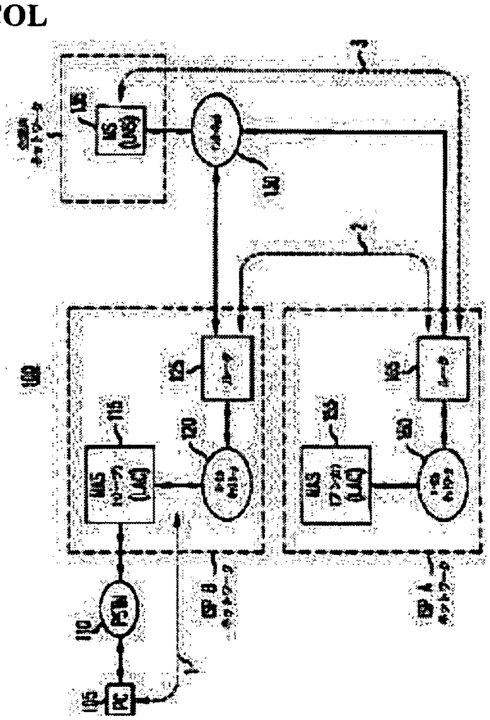
(21)Application number : **11-126563**
(22)Date of filing : **07.05.1999**

(71)Applicant : **LUCENT TECHNOL INC**
(72)Inventor : **CHUAH MOOI CHOO**
RAI GIRISH

(30)Priority
Priority number : **98 74745** Priority date : **08.05.1998** Priority country : **US**

(54) **MULTIPLE HOP POINT-TO-POINT PROTOCOL**

(57)Abstract:
PROBLEM TO BE SOLVED: To enable a remote user to perform access through an internet service provider(ISP) under visiting to a virtual private network in addition to a home ISP by establishing a multiple hop packet tunnel with another packet terminal and repeating a message with the other packet terminal through the multiple hop packet tunnel.
SOLUTION: A communication system 100 shows the multiple hop tunnel, one hop comes from an ISP B network to an ISP A network and the other hop comes from the ISP A network to the network of a company. The tunnel and call are established between a serve LAC 115 and an anchor LAC 155. Similarly, the tunnel and call are established between the anchor LAC 155 and an LSN 135. When the tunnel is established, a lot of control message transactions are generated and a point-to-point protocol is set.



(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－355272

(43)公開日　平成11年(1999)12月24日

(51)Int.Cl.⁶	識別記号	ＦＩ	
Ｈ０４Ｌ　12/22		Ｈ０４Ｌ　11/26	
12/56		11/20	１０２Ａ

審査請求　未請求　請求項の数14　ＯＬ　（全 19 頁）

(21)出願番号　特願平11－126563

(22)出願日　平成11年(1999) 5月7日

(31)優先権主張番号　０９／０７４７４５

(32)優先日　1998年5月8日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　596092698
ルーセント　テクノロジーズ　インコーポレーテッド
アメリカ合衆国．07974－0636　ニュージャーシィ，マレイ　ヒル，マウンテン　アヴェニュー　600

(72)発明者　ムーイ　チョー　チュー
アメリカ合衆国　07724　ニュージャーシィ，イートンタウン，イートンクレスト　ドライヴ　148ビー

(74)代理人　弁理士　岡部　正夫　（外11名）

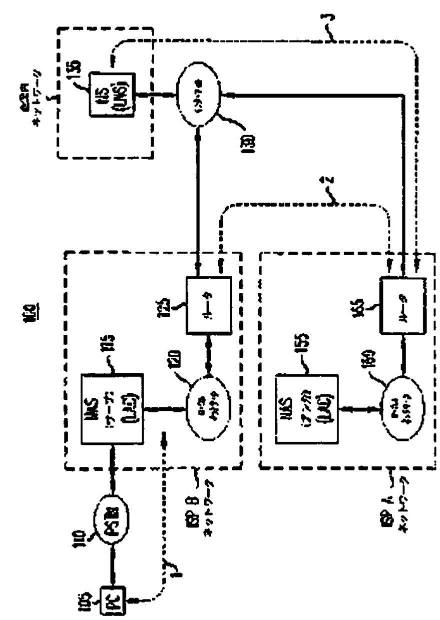
最終頁に続く

(54)【発明の名称】　多重ホップ・ポイント・ツー・ポイント・プロトコル

(57)【要約】

【課題】　本発明は、通信におけるパケット通信システムに関し、特に多重トンネルによる私設網への遠隔アクセスを可能にする仮想私設網（ＶＰＮ）サービスに関する技術を提供する。

【解決手段】　本発明は、パケット・サーバで使用される方法であって、他のパケット終端間に多重ホップ・パケット・トンネルを確立する段階と、該多重ホップ・パケット・トンネルを通じて該他のパケット終端間でメッセージを中継する段階とからなることを特徴とする。これにより、多数のインターネット・サービス・プロバイダ（ＩＳＰ）を通じて仮想ダイヤルアップ・サービスが提供され、特に、遠隔ユーザはサーブＩＳＰへの接続を確立することによって仮想ダイヤルアップ・サービスにアクセスする。サーブＩＳＰは、アンカＩＳＰへの第１トンネルを確立する。アンカＩＳＰは、例えば、私設イントラネットへのトンネルを確立する。その結果、多重トンネルによる私設網への遠隔アクセスを可能にする仮想私設網（ＶＰＮ）サービスが提供される。



PATENT ABSTRACTS OF JAPAN

(11)Publication number : **09-275404**
(43)Date of publication of application : **21.10.1997**

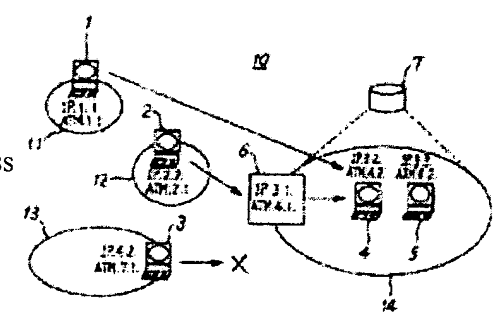
(51)Int.Cl. H04L 12/28
H04L 12/46
H04L 29/06

(21)Application number : **08-083518**
(22)Date of filing : **05.04.1996**

(71)Applicant : **NIPPON TELEGR & TELEPH CORP <NTT>**
(72)Inventor : **MURAYAMA JUNICHI**
TANIMOTO SHIGEAKI
ISHIHARA FUMIAKI
OZAWA KAZUYUKI

(54) ADDRESS SOLUTION PROCESSING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an address solution processing method in which an intensified security function and high speed communication are made compatible.
SOLUTION: In the method for solving a physical address of a non-multiple address wide area network 10 from an internet address by an address solution server 7 used to build up an internet on the non-multiple address wide area network 10, in the case of receiving an address solution request with respect to a same destination internet address, a reply is made or not by a different physical address depending on the internet address of a request source for address solution. In the embodiment, based on information registered in advance, a reply is made by a physical address of a destination host with respect to an address solution request from a host whose communication is allowed and no reply is made to an address solution request from a host whose communication is not allowed, and reply is made with a physical address of a router having a security function with respect to an address solution request from a host whose communication permission is not definitely decided.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－275404

(43)公開日　平成９年(1997)10月21日

(51)Int.Cl.⁶	識別記号	庁内整理番号	F I		技術表示箇所
H04L 12/28		9466-5K	H04L 11/20	D	
12/46			11/00	310C	
29/06			13/00	305Z	

審査請求 未請求 請求項の数２ ＯＬ（全 ４ 頁）

(21)出願番号　特願平8－83518

(22)出願日　平成８年(1996)４月５日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　村山　純一
東京都新宿区西新宿３丁目19番２号　日本電信電話株式会社内

(72)発明者　谷本　茂明
東京都新宿区西新宿３丁目19番２号　日本電信電話株式会社内

(72)発明者　石原　文明
東京都新宿区西新宿３丁目19番２号　日本電信電話株式会社内

(74)代理人　弁理士　杉村　暁秀　（外１名）

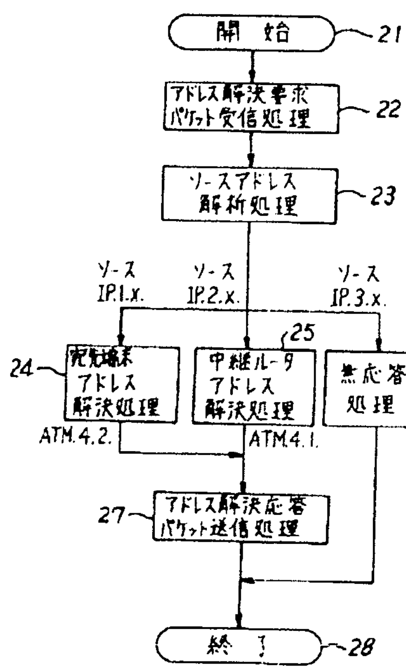
最終頁に続く

(54)【発明の名称】　アドレス解決処理方法

(57)【要約】

【課題】　セキュリティ機能の強化と高速通信とが両立したアドレス解決処理方法を提供する。

【解決手段】　非同報型広域網上にインタネットを構築する際に用いるアドレス解決サーバで、インタネットアドレスから非同報型広域網の物理アドレスを解決する方法において、同一宛先インタネットアドレスに対するアドレス解決要求受信時に、アドレス解決の要求元のインタネットアドレスに応じて異なる物理アドレスで応答するか又は応答しないようにする。一例では、予め登録された情報に基づき、通信許可済のホストからのアドレス解決要求に対しては宛先ホストの物理アドレスで応答し、通信不許可のホストからのアドレス解決要求に対しては応答せず、通信許可又は不許可を一律に決められないホストからのアドレス解決要求に対してはセキュリティ機能を有する中継ルータの物理アドレスで応答する。



【特許請求の範囲】

【請求項1】　非同報型広域網上にインタネットを構築する際に用いられるアドレス解決サーバで、インタネットで用いられるインタネットアドレスから非同報型広域網で用いられる物理アドレスを解決するアドレス解決処理方法において、同一宛先インタネットアドレスに対するアドレス解決要求受信時に、アドレス解決の要求元のインタネットアドレスに応じて異なる物理アドレスで応答するか又は応答しないことを特徴とするアドレス解決処理方法。

【請求項2】　予め登録された情報に基づき、通信を許可されているホストからのアドレス解決要求に対しては宛先ホストの物理アドレスで応答し、通信を許可されていないホストからのアドレス解決要求に対しては応答せず、通信の許可又は不許可を一律に決められないホストからのアドレス解決要求に対してはセキュリティ機能を有する中継ルータの物理アドレスで応答することを特徴とする請求項1に記載のアドレス解決処理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、非同報型広域網上にインタネットを構築する際に用いられるアドレス解決サーバに用いて好適なアドレス解決処理方法に関するものである。

【0002】非同報型広域網上でのアドレス解決処理は、非同報型広域網上の異なるサブネットに帰属するホスト間で、中継ルータを介さない高速パケット通信経路を設定するために必要な処理である。これを実現する従来のアドレス解決処理方法では、同一宛先インタネットアドレスに対するアドレス解決要求に対しては、アドレス解決の要求元のインタネットアドレスに関わりなく、同一の物理アドレスで応答していた。

【0003】

【発明が解決しようとする課題】非同報型広域網上に構築されたインタネットでは、異なるサブネットに帰属するホスト間通信でも中継ルータを介さない通信が可能であるため、同一宛先インタネットアドレスに対するアドレス解決要求に対して、アドレス解決の要求元のインタネットアドレスに関わりなく同一の物理アドレスで応答すると、常に中継ルータを介しない通信が行われてしまう。中継ルータを介さない通信が行われると、パケット中継処理遅延を削減できるものの、パケット転送路上でファイアウォールと呼ばれるようなパケット中継装置を用いてパケットフィルタリングを行うことが不可能になる。

【0004】一方この問題を解決するために、常に中継ルータを介した通信を行うこともできるが、この場合、パケット転送路上でパケットフィルタリングを行うことが可能になるものの、常にパケット中継処理遅延が増加する。従って、このような従来のアドレス解決処理方法では、セキュリティ機能の弱い高速通信又はセキュリティ機能の強い低速通信のいずれかしか実現できないという欠点があった。

【0005】そこで、本発明はこの問題を解決し、セキュリティ機能の強化と高速通信とを両立させるアドレス解決処理方法を提供することを目的とする。

【0006】

【課題を解決するための手段】本発明のアドレス解決処理方法は、上述の目的を達成するために行われた発明であって、パケット転送に先立つアドレス解決処理時に、同一宛先インタネットアドレスに対するアドレス解決要求受信時でも、アドレス解決の要求元のインタネットアドレスに応じて異なる物理アドレスで応答するか又は応答しないことを特徴とする。

【0007】このような本発明においては、アドレス解決処理時に、例えば、予め登録された情報に基づき、通信を許可されているホストからのアドレス解決要求に対しては直接宛先ホストの物理アドレスで応答し、通信を許可されていないホストからのアドレス解決要求に対しては応答せず、通信の許可又は不許可を一律に決められないホストからのアドレス解決要求に対してはセキュリティ機能を有する中継ルータの物理アドレスで応答するようにすることができる。

【0008】このようにすれば、通信を許可されているホストとは高速通信が実現され、通信を許可されていないホストからのアクセスが防止され、通信の許可又は不許可を一律に決められないホストとは、セキュリティ機能を有する中継ルータを介した通信が実現され、セキュリティ機能の強化と高速通信とを両立させることができる。

【0009】

【発明の実施の形態】次に図面を用いて、本発明の実施例を説明する。図1は本発明を実施するためのネットワークモデルを示す図、図2はアドレス解決サーバでの本発明におけるアドレス解決処理を説明するフローチャートである。

【0010】図1のネットワークモデルは広域ＡＴＭ網10を示しており、この広域ＡＴＭ網10は、端末1を含むサブネット11、端末2を含むサブネット12、端末3を含むサブネット13、並びに、端末4、端末5、ルータ6及びアドレス解決サーバ7を含むサブネット14から構成されている。図中のIP.a.b. はインタネットアドレスを示し、ATM.a.b.は非同報型広域網の物理アドレスを意味し、ａの部分はサブネット部、ｂの部分はホスト部を表す。また、図中のｘは任意の正の整数を表す。このような構成において、例えば、アドレス解決サーバ7には、予め、ルータ6を介さない通信を許可するサブネットとしてサブネット11を、通信を許可しないサブネットとしてサブネット13を登録する。

【0011】先ず、ルータを介さない通信を許可する場

合について説明する。サブネット11の端末1がサブネット14の端末4と通信しようとした場合、端末1はアドレス解決サーバ7にアドレス解決要求パケットを送信する。アドレス解決サーバ7は、アドレス解決要求パケット受信処理を行い（図2のステップ22）、この後ソースアドレス解析処理を行い（ステップ23）端末1のIP.1.1.を特定する。IP.1.1.はルータを介さない通信を許可するサブネット1（IP.1.x）に帰属するため、宛先端末アドレス解析処理を行い（ステップ24）、ATM.4.2 を解決する。

【0012】この後アドレス解決応答パケット送信処理を行い（ステップ27）、アドレス解決要求パケット送信元の端末1に対してATM.4.2 を解決したアドレス解決応答パケットを送り返す。アドレス解決終了後、端末1はIPパケットをATM.4.2 を付与した内部転送用フレームにカプセル化し、これを直接端末4に転送する。なお、図2のステップ21及び28は、それぞれ開始及び終了のステップである。

【0013】次に、通信を許可しない場合について説明する。サブネット13の端末3がサブネット14の端末4と通信しようとした場合、端末3はアドレス解決サーバ7にアドレス解決要求パケットを送信する。アドレス解決サーバ7は、アドレス解決要求パケット受信処理を行い（図2のステップ22）、この後ソースアドレス解析処理を行い（ステップ23）、端末1のIP.4.2. を特定する。IP.4.2. は通信を許可しないサブネット13（IP.4.x）に帰属するため、無応答処理を行い（ステップ26）、ここで処理が終了する。ここでは、アドレス解決が行われないため、端末3はIPパケットを端末4に向けて送信できない。

【0014】最後に通信の許可又は不許可が不明な場合について説明する。サブネット12の端末2がサブネット14の端末4と通信しようとした場合、端末2はアドレス解決サーバ7にアドレス解決要求パケットを送信する。アドレス解決サーバ7は、アドレス解決要求パケット受信処理を行い（図2のステップ22）、この後ソースアドレス解析処理を行い（ステップ23）、端末1のIP.2.2. を特定する。IP.2.2.の端末に関しては許可又は不許可が不明のため、中継ルータアドレス解決処理を行い（ステップ25）、ATM.4.1 を解決する。

【0015】この後アドレス解決応答パケット送信処理を行い（ステップ27）、アドレス解決要求パケット送信元の端末2に対してATM.4.1 を解決したアドレス解決応答パケットを送り返す。アドレス解決終了後、端末2はIPパケットをATM.4.1 を付与した内部転送用フレームにカプセル化し、これを中継ルータ6に転送する。中継ルータ6では、中継パケットのソースIPアドレス又は TCPポート番号等を基にしてパケットフィルタリングを行い、必要なパケットのみを端末4に転送する。

【0016】

【発明の効果】上述のように、本発明によれば、アドレス解決処理時におけるセキュリティ機能及びパケット転送時におけるセキュリティ機能が効果的に発揮される。即ち、アドレス解決処理時におけるセキュリティ機能によって、通信を許可されているホストとは中継ルータを介さない高速通信が実現され、通信を許可されていないホストからのアクセスが防止され、通信の許可又は不許可を一律に決められないホストとはセキュリティ機能を有する中継ルータを介した通信が実現される。また、パケット転送時のセキュリティ機能によって、通信の許可又は不許可を一律に決められないホストとの通信時に、中継ルータにおいて、中継パケットのソースIPアドレス又は TCPポート番号等を基にしてパケットフィルタリングを行うことができる。従って、セキュリティ機能の強化と高速通信とを両立させることができる。

【図面の簡単な説明】

【図1】本発明を実施するためのネットワークモデルを示す図である。

【図2】アドレス解決サーバでの本発明におけるアドレス解決処理を説明するフローチャートである。

【符号の説明】

1、2、3、4、5　端末

6　ルータ

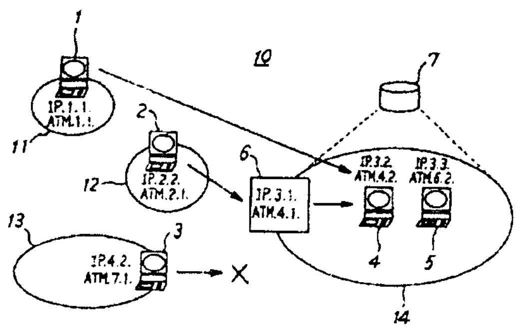
7　アドレス解決サーバ

10　広域ATM網

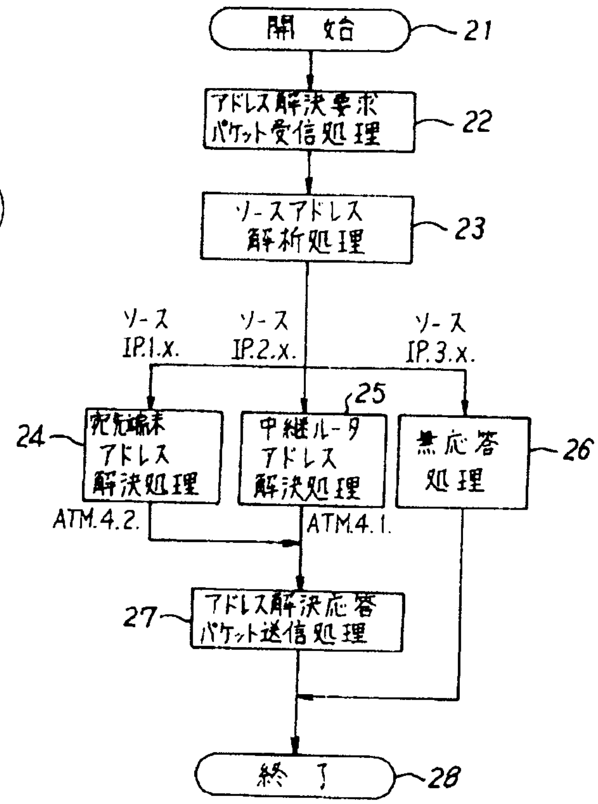
11、12、13、14　サブネット

21～28　フローチャートの各ステップ

【図1】



【図2】



フロントページの続き

(72)発明者　小澤　和幸
東京都新宿区西新宿3丁目19番2号　日本電信電話株式会社内

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 29/00	A2	(11) International Publication Number: WO 00/14938 (43) International Publication Date: 16 March 2000 (16.03.00)

(21) International Application Number: PCT/US99/20158

(22) International Filing Date: 1 September 1999 (01.09.99)

(30) Priority Data:
09/150,630 9 September 1998 (09.09.98) US

(71) Applicant: SUN MICROSYSTEMS, INC. [US/US]; 901 San Antonio Road, M/S PAL01-521, Palo Alto, CA 94303 (US).

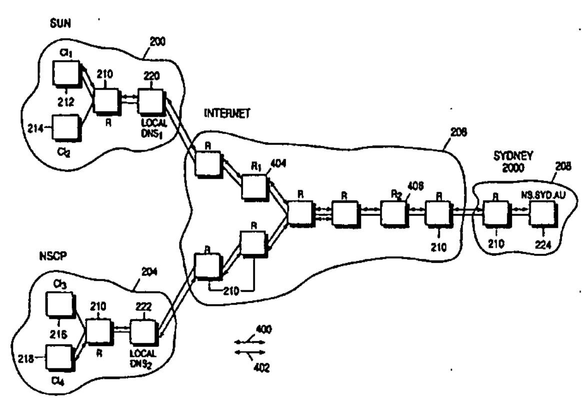
(72) Inventors: GUPTA, Amit; Apartment J207, 2000 Walnut Avenue, Fremont, CA 94538 (US). SCHUBA, Christoph; 473 Hope Street #1, Mountain View, CA 94041 (US). BAEHR, Geoffrey; 531 Colorado AVenue, Palo Alto, CA 94306 (US).

(74) Agents: HECKER, Gary, A. et al.; Hecker & Harriman, Suite 2300, 1925 Century Park East, Los Angeles, CA 90067 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, 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, 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
Without international search report and to be republished upon receipt of that report.

(54) Title: METHOD AND APPARATUS FOR TRANSPARENTLY PROCESSING DNS TRAFFIC



(57) Abstract

A method and apparatus for transparently processing DNS traffic. To access information on the internet using a domain name, the internet protocol (IP) address that maps to the host name must be determined. The host name system (DNS) is utilized to transmit and process the address and domain name information. DNS traffic comprises approximately 10 % of the internet network traffic. When a client requests a name server to translate a domain name into an IP address, the requests are forwarded from one network router to another network router until a name server that maintains the desired information is reached. The network routers do not examine the information, but merely forward the information along the pathway to the destination name server. One or more embodiments of the invention provide for updated routers that recognize when the information consists of DNS traffic, parses the information, caches the address information (if any), and then continues to forward the desired information back to the client of the name service. Consequently, when another request for similar address information is forwarded to a router, the router can provide the response to the requestor instead of forwarding the request to a distant name server. In this manner, routers intercept DNS traffic and cache DNS information, allowing clients that utilize different name servers to benefit from the cached information. Such updated routers reduce the latency in DNS responses and reduce network traffic.

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 AND APPARATUS FOR TRANSPARENTLY PROCESSING DNS TRAFFIC

BACKGROUND OF THE INVENTION

1. FIELD OF THE INVENTION

This invention relates to the field of computer software, and, more specifically, to caching DNS information.

2. BACKGROUND ART

In a computer network environment and the internet, computers on the network (clients or servers) are assigned unique identifiers that may be mapped to a textual name referred to as a domain name. Computer users often only have knowledge of the domain name and not the unique identifier. To communicate with a computer on the network, the unique identifier of the computer you are contacting must be ascertained. To ascertain the unique identifier, network routers forward the identifier request to other routers until a domain name server that maintains the desired information is located. Existing schemes can waste time forwarding the identifier request from one router to another router resulting in an increase of traffic on the network and slowing down the time it takes to access and retrieve any information on the internet. These problems can be understood by reviewing networks, internets, and how they work.

Networks

In modern computing environments, it is commonplace to employ multiple computers or workstations linked together in a network to communicate between, and share data with, network users. A network also may include resources, such as printers, modems, file servers, etc., and may also include services, such as electronic mail.

A network can be a small system that is physically connected by cables (a local area network or "LAN"), or several separate networks can be connected together to form a larger network (a wide area network or "WAN"). Other types of networks include the internet, tel-com networks, the World Wide Web, intranets, extranets, wireless networks, and other networks over which electronic, digital, and/or analog data may be communicated.

Computer systems sometimes rely on a server computer system to provide information to requesting computers on a network. When there are a large number of requesting computers, it may be necessary to have more than one server computer system to handle the requests. In prior art systems, there is a problem in efficiently directing requests to the correct server in a multiple server system.

One area where this has been a problem is on the internet. The problem can be better understood by reviewing the structure and operation of the internet below.

The Internet

The Internet is a worldwide network of interconnected computers. An Internet client accesses a computer on the network via an Internet provider. An Internet provider is an organization that provides a client (e.g., an individual or other organization) with access to the Internet (via analog telephone line or Integrated Services Digital Network line, for example). A client can, for example, read information from, download a file from or send an electronic mail message to another computer/client using the Internet.

To retrieve a file or service on the Internet, a client must search for the file or service, make a connection to the computer on which the file or service is stored, and download the file or service. Each of these steps may involve a separate application and access to multiple, dissimilar computer systems. The World Wide Web (WWW) was developed to provide a simpler, more uniform means for accessing information on the Internet.

The components of the WWW include browser software, network links, servers. and WWW protocols. The browser software, or browser, is a user-friendly interface (i.e., front-end) that simplifies access to the Internet. A browser allows a client to communicate a request without having to learn a complicated command syntax, for example. A browser typically provides a graphical user interface (GUI) for displaying information and receiving input. Examples of browsers currently available include Mosaic, Netscape Navigator and Communicator, Microsoft Internet Explorer, and Cello.

Information servers maintain the information on the WWW and are capable of processing a client request. Hypertext Transport Protocol (HTTP) is the standard protocol for communication with an information server on the WWW. HTTP has communication methods that allow clients to request data from a server and send information to the server.

To submit a request, the client contacts the HTTP server and transmits the request to the HTTP server. The request contains the communication method requested for the transaction (e.g., GET an object from the server or POST data to an object on the server). The HTTP server responds to the client by sending a status of the request and the requested information. The connection is then terminated between the client and the HTTP server.

A client request therefore, consists of establishing a connection between the client and the HTTP server, performing the request, and terminating the connection. The HTTP server does not retain any information about the request after the connection has been terminated. HTTP is, therefore, a stateless protocol. That is, a client can make several requests of an HTTP server, but each individual request is treated independent of any other request. The server has no recollection of any previous request.

An addressing scheme is employed to identify Internet resources (e.g., HTTP server, file or program). This addressing scheme is called Uniform Resource Locator (URL). A URL contains the protocol to use when accessing the server (e.g., HTTP), the Internet domain name of the site on which the server is running, the port number of the server, and the location of the resource in the file structure of the server.

The WWW uses a concept known as hypertext. Hypertext provides the ability to create links within a document to move directly to other information. To activate the link, it is only necessary to click on the hypertext link (e.g., a word or phrase). The hypertext link can be to information stored on a different site than the one that supplied the current information. A URL is associated with the link to identify the location of the additional information. When the link is activated, the client's browser uses the link to access the data at the site specified in the URL.

If the client request is for a file, the HTTP server locates the file and sends it to the client. An HTTP server also has the ability to delegate work to gateway programs. The Common Gateway Interface (CGI) specification defines a mechanism by which HTTP servers communicate with gateway programs. A gateway program is referenced using a URL. The HTTP server activates the program specified in the URL and uses CGI mechanisms to pass program data sent by the client to the gateway program. Data is passed from the server to the gateway program via command-line arguments, standard input, or environment variables. The gateway program processes the data and returns its response to the server using CGI (via standard input, for example). The server forwards the data to the client using the HTTP.

A browser displays information to a client/user as pages or documents (referred to as "web pages" or "web sites"). A language is used to define the format for a page to be displayed in the WWW. The language is called Hypertext Markup Language (HTML). A WWW page is transmitted to a client as an HTML document. The browser executing at the client parses the document and displays a page based on the information in the HTML document.

HTML is a structural language that is comprised of HTML elements that are nested within each other. An HTML document is a text file in which certain strings of characters, called tags, mark regions of the document and assign special meaning to them. These regions are called HTML elements. Each element has a name, or tag. An element can have attributes that specify properties of the element. Blocks or components include unordered list, text boxes, check boxes, radio buttons, for example. Each block has properties such as name, type, and value. The following provides an example of the structure of an HTML document:

```
<HTML>
        <HEAD>
        .... element(s) valid in the document head
        </HEAD>
        <BODY>
        .... element(s) valid in the document body
        </BODY>
</HTML>
```

Each HTML element is delimited by the pair of characters "<" and ">". The name of the HTML element is contained within the delimiting characters. The combination of the name and delimiting characters is referred to as a marker, or tag. Each element is identified by its marker. In most cases, each element has a start and ending marker. The ending marker is identified by the inclusion of an another character, "/" that follows the "<" character.

HTML is a hierarchical language. With the exception of the HTML element, all other elements are contained within another element. The HTML element encompasses the entire document. It identifies the enclosed text as an HTML document. The HEAD element is contained within the HTML element and includes information about the HTML document. The BODY element is contained within the HTML. The BODY element contains all of the text and other information to be displayed. Other HTML elements are described in HTML reference manuals.

Domain Name Server

A computer user navigates the internet or web from a browser on a computer system. To access a web site, the user enters the host name (or domain name) of the web site into the browser. This can be accomplished by clicking on a link, by activating a tool bar button, or by manually entering a name or address into a location field and pressing "enter". The names that a browser client uses are known as host names, such as www.sun.com for example. The name that is entered is not the actual Internet Protocol (IP) address of the intended web server. The actual IP address is a string of numbers that uniquely locate the web server that provides the web site data. A worldwide distributed database system, called the "Domain Name System (DNS)" provides the mapping between server names and the associated IP addresses.

Each client (or host) is configured with, or otherwise learns about, a name server that is willing to answer its queries (for mapping a domain name to an IP address, or vice versa). Such a name server is referred to as the "local name server" for that host. Client application software, such as a web browser, also use a local library, called the "DNS resolver" to obtain the translation from server name to IP address. The resolver in turn contacts a predetermined local DNS name server to obtain the translation. DNS name servers can maintain caches of previously resolved names. More specifically, name resolution processes typically require two hosts on the client side. Consider a user working on "asha.eng.sun.com" that wants to get the address of "whitehouse.gov". The client browser will talk with a local resolver (a library attached to the browser process itself, in the current example running on asha.eng.sun.com). The local resolver will go to one of a relatively small number of local name servers, e.g. "ns.sun.com". Here ns.sun.com is called the client side name server. The client side name server will communicate with the outside world to determine the IP address of whitehouse.gov, and forward this information to the resolver that is part of the browser process.

DNS is a global network of servers that translate host names into numerical addresses (known as Internet Protocol, or IP addresses) and provides IP address to name mapping as well. A DNS server consists of a name server and a resolver. The name server provides responses to resolver requests when it can by supplying the correct address for the host name supplied by the resolver. Referring to Figure 1, at step 100, the user enters the domain name into the browser. At step 102, the browser requests the DNS Resolver to translate the domain name into the IP address. At step, 104, the resolver searches its cache to see if it already has a valid (unexpired) mapping available. If the cache has a valid mapping, it returns the IP address to the browser at step 116. If the mapping is not in cache, the resolver forwards the request to the local name server at step 106.

All name servers know about at least one other name server that provides the DNS service for the root (.) domain. Thus, at step 108, the local name server contacts the name server for the any known domain. For example, if the host name is "www.java.sun.com", and the local name server does not know the address for the name server "java.sun.com", it will check to see if it knows the next level domain, i.e., the address for "sun.com". If the local name server does not know the address for "sun.com", it will check to see if it knows the address of next level domain, i.e., ".com". If the local name server does not know the address for ".com", it will contact the root name server ".". At step 110, the local name server will obtain the address for the complete domain from the name server contacted (if that name server knows the address). Otherwise, at step 110, the local name server will obtain the address for the next level of the domain from the contacted name server. For example, if the local name server contacted the name server for ".com" and that name server does not know the full address, the ".com" name server will return the domain address for "sun.com". Steps 108 and 110 are then repeated until the complete domain address is obtained. Continuing with the above example, the local name server would contact the "java.com" name server and obtain the address for "java.sun.com". The local name server would then contact the name server for "java.sun.com" and obtain the address for "www.java.sun.com". When a request is made to a name server, there are often many network routers ("routers") that forward the request from one location to another until it reaches the desired name server.

Once an intermediate or complete IP address is obtained, the address is saved in cache so that a future request may be serviced entirely from local cache at step 114. Thus, if a request for an alternative domain is received (e.g., a request for "ftp.sun.com"), the local name server can contact the name server (e.g., "sun.com") directly, without repeating the communication with the root domain server or with intermediate name servers (e.g., the ".com" name server). At step, 116, the IP address is returned to the browser. Once the IP address is known, the browser communicates with the web server at that address to retrieve the requested web page or other information.

The operation of the DNS network is described in:

P.V. Mockapetris "Domain names - concepts and facilities", RFC 1034. Nov 1987.

P.V. Mockapetris "Domain names - implementation and specification", RFC 1035. Nov 1987.

DNS Server Problems

When DNS information is cached in a local name server, the cached information is only available to the clients that access that particular local name server (e.g., clients of the same internet service provider, or members of the same organization). Thus, if two users access different local name servers and each user requests the same IP address, both requests will have to go up the chain of name servers through the various routers, to obtain the needed information.

For example, if two users in different universities in New Zealand were to query the DNS for the IP address of www.sun.com, both of the requests would be serviced by the local name server at ns.sun.com in the United States without any local caching benefit. Figure 2 provides another example of the prior art. Clients Cl_1 212 and Cl_2 214 are part of the SUN network 200 that utilizes local name server DNS_1 220. Clients Cl_3 216 and Cl_4 218 are part on the NSCP network 204 that utilizes local name server DNS_2 222. If client Cl_1 212 requests information regarding an IP address on the SYDNEY 2000 network 208 in Sydney, Australia, the request is processed at the SYDNEY 2000 208 network's local name server ns.syd.au 224. Routers 210 would forward the request from Cl_1 to the local name servers 220 that forwards the request through routers 210 on the internet 206 until it reaches the SYDNEY 2000 network 208 and name server 224. The request is then transmitted back along the same route through routers 210 until it returns back to local name server 220 where it is cached.

Only clients that access that same local DNS name server benefit from the caching information. Thus, in the above example, only Cl_2 benefits from the Cl_1 request and its resulting cached information. If Cl_4 requests a DNS translation for www.syd.au, it does not benefit from the cached information, and the information is requested and transmitted all the way to Australia and back. Thus, both DNS_1 and DNS_2 would obtain the relevant information from Australia creating traffic on the individual networks 200 204 and 208 and internet 206.

Networks may be divided up into layers. For example, one layer may provide for the forwarding of information from one location to another, referred to as the network layer, and another layer may provide for the parsing and processing of the information passed across the network, referred to as the application layer. Name resolution as provided by the domain name system (DNS) is an application layer protocol. Network routers 210 are only concerned with the network layer protocol and forward the DNS request to its desired destination. Consequently, routers 210 don't parse or process the information that they forward in packets.

Network Traffic Reduction

Prior art methods for reducing network traffic have provided methods for caching web pages and HTML information. Two such prior art methods are referred to as Active Networks and Transparent Proxies.

Active Networks

Routers are dedicated machines for forwarding and switching traffic as quickly as possible. In an Active Network, specific routers are configured to process packets of web and other non-DNS information. Specific geographic locations are chosen to place the specially configured routers. Consequently, the performance of an Active Network is based on the placement strategy of the updated routers.

Transparent Proxies

Transparent Proxies are used mostly by large corporations and internet service providers for reducing their web traffic. In a typical set-up, the domain administrator configures the routers so that all of the web requests (identified by a port number, e.g., 80) are automatically diverted to a proxy server ("transparent proxy"). A proxy server (or proxy) is a server that carries out requests transmitted to it (i.e., from a client), keeping copies of fetched documents or information for some time so that they can be accessed more quickly in the future, speeding up access for commonly requested information. This storing and retrieval of information and fetched documents by the proxy is referred to as caching and the information maintained in the proxy is referred to as a cache or proxy cache. If the proxy does not have the desired information, the proxy sends a request to the appropriate web server (which may be processed through several routers) that then returns the information to the proxy for caching. When the proxy gets the desired information, it provides this information to the requesting client.

The prior art methods do not provide any method for optimizing DNS traffic. Approximately 10% of the traffic on the internet is currently comprised of DNS traffic. Further, since DNS information does not change often (IP addresses often remain the same even when computers on a network are moved), the validity of a DNS entry may be much longer than that of data transmitted through the web. Consequently, an efficient method for optimizing and processing DNS traffic is needed.

SUMMARY OF THE INVENTION

A method and apparatus for transparently processing DNS traffic. To access information on the internet using a domain name, the internet protocol (IP) address that maps to the domain name must be determined. The domain name system (DNS) is utilized to transmit and process the address and domain name information. DNS traffic comprises approximately 10% of the internet network traffic.

When a client requests a name server to translate a domain name into an IP address, the requests are forwarded from one network router to another network router until a name server that maintains the desired information is located. The network routers do not examine the information, but merely forward the information along the pathway to the destination name server.

One or more embodiments of the invention provide for updated routers that recognize when the information consists of DNS traffic, parses the information, caches the address information (if any), and then continues to forward the desired information back to the name server. Consequently, when another request for similar address information is forwarded to a router, the router can provide the response to the requestor instead of forwarding the request to a distant name server. In this manner, routers intercept DNS traffic and cache DNS information, allowing clients that utilize different name servers to benefit from the cached information. Such updated routers reduce the latency in DNS responses and reduce network traffic.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 illustrates a prior art method for processing DNS information.

Figure 2 demonstrates the relationship between several networks.

Figure 3 is a block diagram of one embodiment of a computer system capable of providing a suitable execution environment for one or more embodiments of the invention.

Figure 4 demonstrates the relationship between several networks and the path of DNS traffic according to one or more embodiments of the invention.

Figure 5 illustrates the steps executed by an updated router according to one or more embodiments of the invention.

DETAILED DESCRIPTION OF THE INVENTION

The invention is a method and apparatus for transparently caching DNS traffic. In the following description, numerous specific details are set forth to provide a more thorough description of embodiments of the invention. It is apparent, however, to one skilled in the art, that the invention may be practiced without these specific details. In other instances, well known features have not been described in detail so as not to obscure the invention.

Embodiment of Computer Execution Environment (Hardware)

An embodiment of the invention can be implemented as computer software in the form of computer readable code executed on a general purpose computer such as computer 300 illustrated in Figure 3, or in the form of bytecode class files running on such a computer. A keyboard 310 and mouse 311 are coupled to a bi-directional system bus 318. The keyboard and mouse are for introducing user input to the computer system and communicating that user input to processor 313. Other suitable input devices may be used in addition to, or in place of, the mouse 311 and keyboard 310. I/O (input/output) unit 319 coupled to bi-directional system bus 318 represents such I/O elements as a printer, A/V (audio/video) I/O, etc.

Computer 300 includes a video memory 314, main memory 315 and mass storage 312, all coupled to bi-directional system bus 318 along with keyboard 310, mouse 311 and processor 313. The mass storage 312 may include both fixed and removable media, such as magnetic, optical or magnetic optical storage systems or any other available mass storage technology. Bus 318 may contain, for example, thirty-two address lines for addressing video memory 314 or main memory 315. The system bus 318 also includes, for example, a 32-bit data bus for transferring data between and among the components, such as processor 313, main memory 315, video memory 314 and mass storage 312. Alternatively, multiplex data/address lines may be used instead of separate data and address lines.

In one embodiment of the invention, the processor 313 is a microprocessor manufactured by Motorola, such as the 680X0 processor or a microprocessor manufactured by Intel, such as the 80X86, or Pentium processor, or a SPARC microprocessor from Sun Microsystems, Inc. However, any other suitable microprocessor or microcomputer may be utilized. Main memory 315 is comprised of dynamic random access memory (DRAM). Video memory 314 is a dual-ported video random access memory. One port of the video memory 314 is coupled to video amplifier 316. The video amplifier 316 is used to drive the cathode ray tube (CRT) raster monitor 317. Video amplifier 316 is well known in the art and may be implemented by any suitable apparatus. This circuitry converts pixel data stored in video memory 314 to a raster signal suitable for use by monitor 317. Monitor 317 is a type of monitor suitable for displaying graphic images.

Computer 300 may also include a communication interface 320 coupled to bus 318. Communication interface 320 provides a two-way data communication coupling via a network link 321 to a local network 322. For example, if communication interface 320 is an integrated services digital network (ISDN) card or a modem, communication interface 320 provides a data communication connection to the corresponding type of telephone line, which comprises part of network link 321. If communication interface 320 is a local area network (LAN) card, communication interface 320 provides a data communication connection via network link 321 to a compatible LAN. Wireless links are also possible. In any such implementation, communication interface 320 sends and receives electrical, electromagnetic or optical signals which carry digital data streams representing various types of information.

Network link 321 typically provides data communication through one or more networks to other data devices. For example, network link 321 may provide a connection through local network 322 to local server computer 323 or to data equipment operated by an Internet Service Provider (ISP) 324. ISP 324 in turn provides data communication services through the world wide packet data communication network now commonly referred to as the "Internet" 325. Local network 322 and Internet 325 both use electrical, electromagnetic or optical signals which carry digital data streams. The signals through the various networks and the signals on network link 321 and through communication interface 320, which carry the digital data to and from computer 300, are exemplary forms of carrier waves transporting the information.

Computer 300 can send messages and receive data, including program code, through the network(s), network link 321, and communication interface 320. In the Internet example, remote server computer 326 might transmit a requested code for an application program through Internet 325, ISP 324, local network 322 and communication interface 320.

The received code may be executed by processor 313 as it is received, and/or stored in mass storage 312, or other non-volatile storage for later execution. In this manner, computer 300 may obtain application code in the form of a carrier wave.

Application code may be embodied in any form of computer program product. A computer program product comprises a medium configured to store or transport computer readable code, or in which computer readable code may be embedded. Some examples of computer program products are CD-ROM disks, ROM cards, floppy disks, magnetic tapes, computer hard drives, servers on a network, and carrier waves.

The computer systems described above are for purposes of example only. An embodiment of the invention may be implemented in any type of computer system or programming or processing environment.

Embodiment of Software Apparatus for Transparently Caching DNS Traffic

One or more embodiments of the invention may be described by examining the layered model of networking and the peer relationships between the different layers. At the network layer, a peer relationship exists between each router that is connected by some type of wire. At the higher application layer, DNS entities (e.g., DNS resolvers and the local name servers) have a peer relationship with multiple hops in between (e.g., the routers). The routers at the network layer (the hops of the network layer) do not examine the information from application layer protocols. The routers merely transparently transfer the information between DNS clients and DNS servers.

In one or more embodiments of the invention, the layering model of networks is violated. DNS traffic is communicated from one machine to another machine through the use of name service ports. DNS traffic commonly arrives from and is transmitted to a specific DNS port (e.g., port 53). Consequently, based on the port information that is present in all IP packets, the routers have the ability to identify when DNS traffic is being transmitted versus when web or other traffic is being transmitted.

When an intermediate router (or hop in the network protocol layer) identifies that DNS information is in the packet it is transmitting across the internet, the routers violate the layering model and examine the information in the packet as if the router were a member of the application protocol. The information is then parsed and cached. Thus, the routers snoop on the DNS replies from a name-server and cache the intercepted replies. The routers also intercept DNS requests, and determine if the request can be served from the cache. If the cache contains the requested information, the router provides the response to the DNS query. If the cache does not contain the requested information, the router forwards the request to the next router or hop along the path to the name server.

Referring to the prior art system of Figure 1, at step 106, the resolver forwards the request to the local name server, and at step 108, the name server of the lowest level domain name is contacted. In one or more embodiments of the invention, the forwarding step 106 and the contacting step 108 are processed through routers that may intercept the transmissions. The routers examine the packet of information from the intercepted transmissions and store any necessary information in cache. Further, when the information is obtained from the name server and transmitted back to the local name server at step 110, in one or more embodiments of the invention, the routers again intercept the transmission, parse the information, and cache the address information as it passes by on its way to the local name server.

Figure 5 demonstrates the process performed by an updated router according to one or more embodiments of the invention. The process starts at step 500. At step 502, the router examines the port information to determine if the current information is DNS traffic or some other type of traffic (e.g., web traffic). If the information is not DNS traffic, the router merely performs as normal and forwards the request to the next hop to its destination at step 512.

If the information is DNS traffic, the router parses the information at step 504. At step 506, the router determines if the parsed information (e.g., the requested address information) is in its cache. If the information is not in its cache, the router stores the relevant information (if any) in its cache at step 510 and forwards the request to the next hop in the information's path at step 512. If the information is in the router's cache, the router returns the requested information to the requestor at step 508. In this manner, the updated routers maintain their own cache and are capable of processing DNS translation requests.

Alternatively, between step 502 and step 504, if the information is DNS traffic, the router will automatically forward the DNS information to a preconfigured host. Routers are currently configured to recognize types of internet traffic and forward specified types of internet traffic to a specific location or host. Once the host receives the information, the host executes the remaining steps 504-514. For example, the host parses the information at step 504 and searches its own cache for valid information at step 506. If there is any information to store in the cache (i.e., the DNS information is being returned), the information is stored in the host's cache at step 510. In such an embodiment, the router classifies and diverts packets to the configured host, and the host performs all additional functionality.

Referring to Figure 4, in one or more embodiments of the invention, one or more of the routers 210 may be modified as defined in Figure 4, to intercept, parse, and cache DNS information. For example, routers 404 and 406 may be updated. Consequently, when Cl_1 212 requests a DNS translation from ns.syd.au 224, the request is forwarded through route 400 along routers 210 and updated routers 404 and 406. However, updated router 404 determines that it is DNS traffic, violates its network layer, and intercepts the request. Router 404 parses the requested information and determines if it is in its cache. If the requested information is in its cache, router 404 returns the result back to Cl_1 212 (along route 400). If the requested information is not in its cache, it merely forwards the request to the next hop in pathway 400. Router 406, upon determining that the transmission is DNS traffic, intercepts the request and searches its cache. Upon determining that the relevant information is not in its cache, router 406 forwards the request to the next hop in pathway 400. The request is forwarded until it reaches the local name server ns.syd.au 224. Alternatively, as described above, in one or more embodiments, the router forwards the request (if it is DNS traffic) to a configured host that maintains the cache and processing capabilities.

The request is processed by ns.syd.au 224 and returned back to Cl_1 212 along path 400. When the information reaches router 406 on its way back to

Cl1 212, router 406 intercepts the request, the router or configured host parses the address information, and stores the address information in cache. Router 406 then forwards the results to the next hop along path 400. Each updated router or configured host along path 400 will store the result in its cache.

Subsequent to the above request, if Cl4 requests a similar DNS translation, the request would be forwarded along route 402. However, router 406 would identify the request as DNS traffic, router 406 intercepts the request, router 406 or a configured host parses the request, searches cache, and returns the requested information back to the previous hop on pathway 402. Consequently, the request by Cl4 is serviced locally at router 406 or the configured host and does not need to be serviced in Australia at ns.syd.au 224.

As described above, according to one or more embodiments of the invention, the updated routers perform additional processing from other routers. The processing by the routers as described above and illustrated in Figure 5, includes viewing a portion of the DNS traffic, parsing the information, maintaining a database for cache storage, and searching cache for the information.

Some DNS name servers return different answers for client requests for the same host name. Such a response may be based on load-balancing considerations (e.g., the attempt to balance network traffic across multiple servers), or it may be chosen to direct the clients to "nearby" hosts. Use of such schemes may be less effective with the transparent DNS caching according to one or more embodiments of the invention. Some schemes provide for strategic geographic placement of cacheable data (e.g., routers that may cache web traffic) in order to provide the information for the highest number of clients possible. The geographical scheme described in pending patent application number 09/081,860 entitled "Method and Apparatus for Effective Traffic Localization Through Domain Name System" which is hereby incorporated by reference, works well when used to determine which network routers are to be updated in accordance with one or more embodiments of the invention. In such a geographic scheme, the information returned is deliberately provided to be applicable to a large number of (if not all) DNS clients, with client-side computation to still achieve the load-balancing and traffic localization goals desired. Such a scenario reduces the network load as well as the latency observed in DNS translations.

Thus, a method and apparatus for encoding content characteristics for the retrieval of information is described in conjunction with one or more specific embodiments. The invention is defined by the claims and their full scope of equivalents.

CLAIMS

1. A method for transparently processing DNS traffic comprising:

transmitting a request for information to a network router;

parsing said transmitted request;

searching cache for said requested information; and

returning said requested information if said requested information is in said cache.

2. The method of claim 1 further comprising:

forwarding said request to a next hop of said request if said requested information is not in said cache;

receiving said requested information;

parsing said requested information;

storing said requested information in said cache; and

forwarding said requested information to a next hop of said requested information.

3. The method of claim 1 wherein said information is internet protocol address information.

4. The method of claim 1 wherein said network router is applicable to one or more DNS clients based on geographical placement.

5. The method of claim 2 wherein said receiving step comprises transmitting said requested information from a name server.

6. A system comprising

a processor;

a memory coupled to said processor;

code executed by said processor configured to transparently process DNS traffic;

said code comprising:

a method transmitting a request for information to a network router;

a method parsing said transmitted request;

a method searching cache for said requested information; and

a method returning said requested information if said requested information is in said cache.

7. The system of claim 6 wherein said code further comprises:

a method forwarding said request to a next hop of said request if said requested information is not in said cache;

a method receiving said requested information;

a method parsing said requested information;

a method storing said requested information in said cache; and

a method forwarding said requested information to a next hop of said requested information.

8. The system of claim 6 wherein said information is internet protocol address information.

9. The system of claim 6 wherein said network router is applicable to one or more DNS clients based on geographical placement.

10. The system of claim 7 wherein said code for a method receiving said requested information comprises a method transmitting said requested information from a name server.

11. A computer program product comprising

a computer usable medium having computer readable program code embodied therein configured to transparently process DNS traffic, said computer program product comprising:

computer readable code configured to cause a computer to transmit a request for information to a network router;

computer readable code configured to cause a computer to parse said transmitted request;

computer readable code configured to cause a computer to search cache for said requested information; and

computer readable code configured to cause a computer to return said requested information if said requested information is in said cache.

12. The computer program product of claim 11 further comprising:

computer readable code configured to cause a computer to forward said request to a next hop of said request if said requested information is not in said cache;

computer readable code configured to cause a computer to receive said requested information;

computer readable code configured to cause a computer to parse said requested information;

computer readable code configured to cause a computer to store said requested information in said cache; and

computer readable code configured to cause a computer to forward said requested information to a next hop of said requested information.

13. The computer program product of claim 11 wherein said information is internet protocol address information.

14. The computer program product of claim 11 wherein said network router is applicable to one or more DNS clients based on geographical placement.

15. The computer program product of claim 12 wherein said computer readable code configured to cause a computer to receive comprises computer readable code configured to cause a computer to transmit said requested information from a name server.

16. The method of claim 1 wherein said cache is maintained by said network router.

17. The method of claim 1 wherein said cache is maintained by a configured host.

18. The system of claim 6 wherein said cache is maintained by said network router.

19. The system of claim 6 wherein said cache is maintained by a configured host.

20. The computer program product of claim 11 wherein said cache is maintained by said network router.

21. The computer program product of claim 11 wherein said cache is maintained by a configured host.

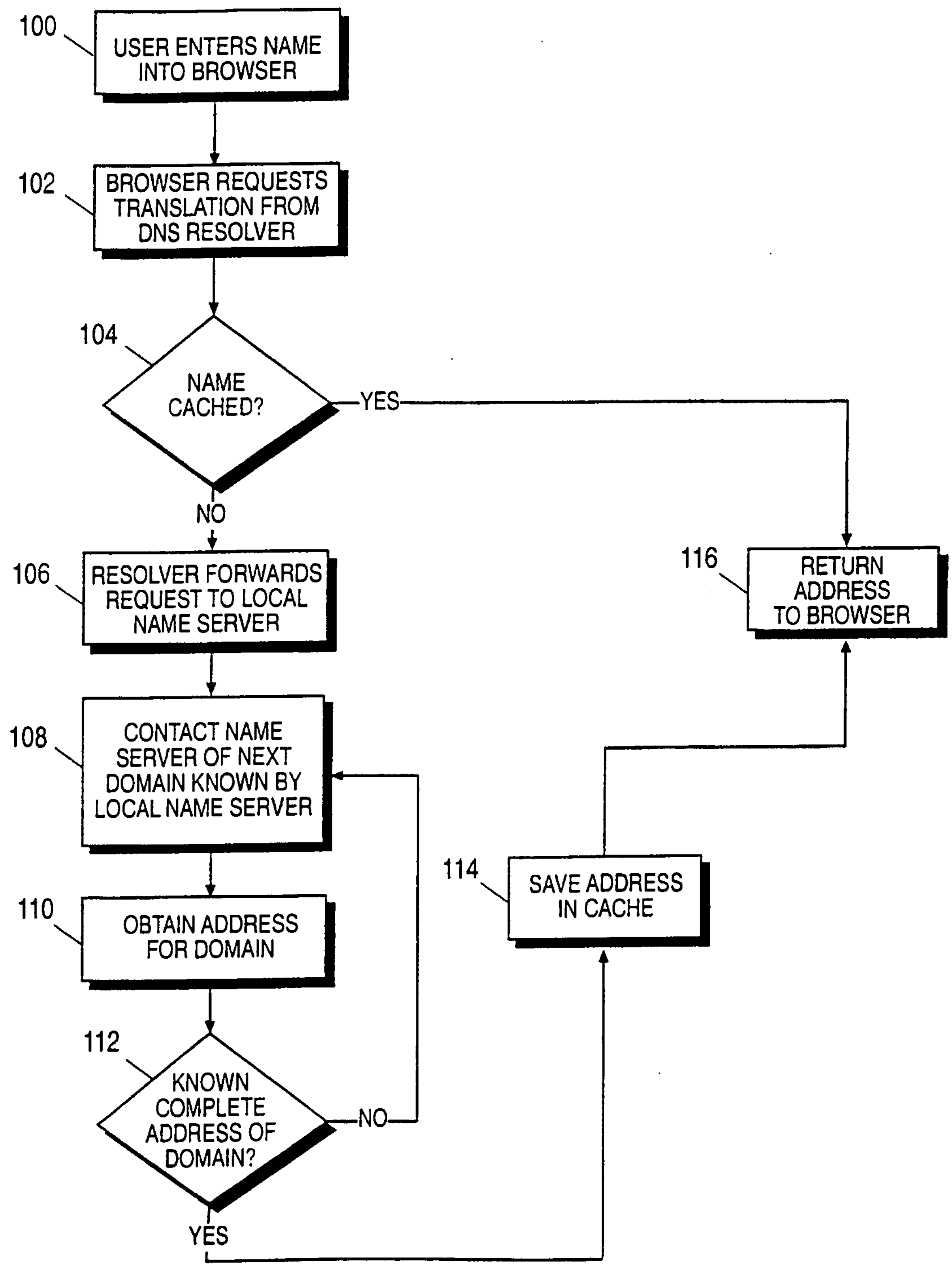

100
USER ENTERS NAME INTO BROWSER
102
BROWSER REQUESTS TRANSLATION FROM DNS RESOLVER
104
NAME CACHED?
YES
NO
106
RESOLVER FORWARDS REQUEST TO LOCAL NAME SERVER
108
CONTACT NAME SERVER OF NEXT DOMAIN KNOWN BY LOCAL NAME SERVER
110
OBTAIN ADDRESS FOR DOMAIN
112
KNOWN COMPLETE ADDRESS OF DOMAIN?
NO
YES
114
SAVE ADDRESS IN CACHE
116
RETURN ADDRESS TO BROWSER

FIG. 1

2/5

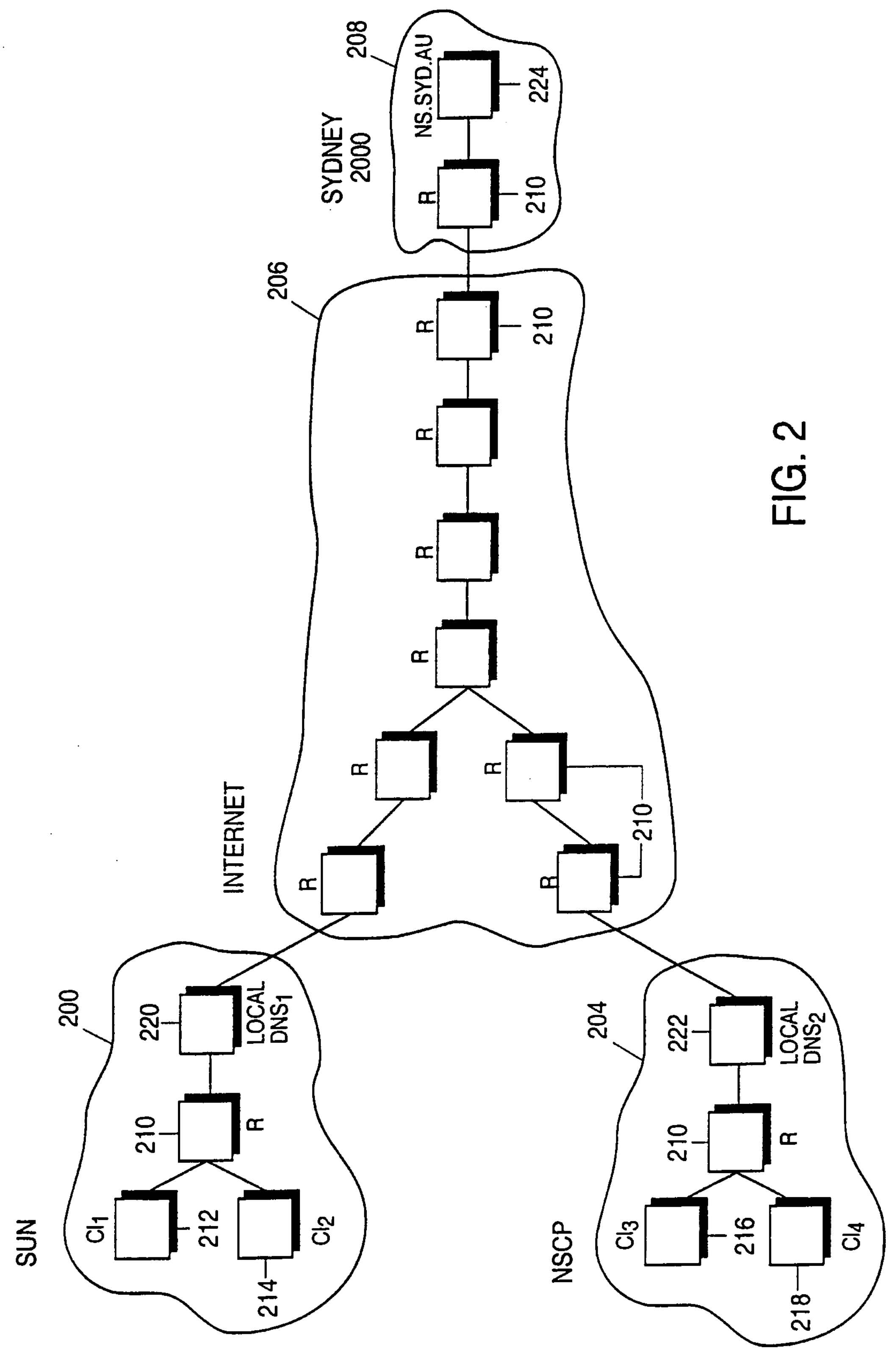


FIG. 2

SUBSTITUTE SHEET (RULE 26)

3/5

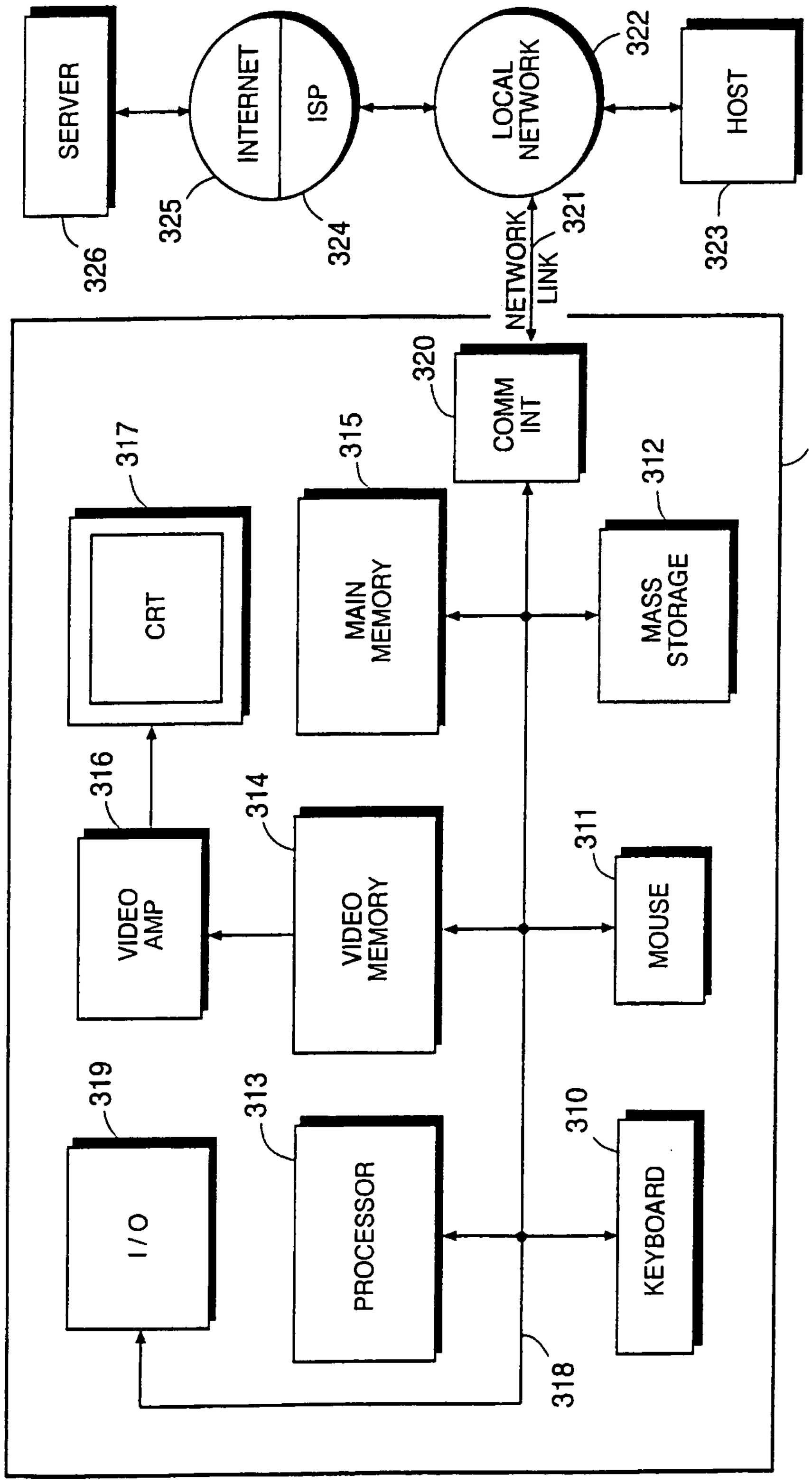

SERVER
INTERNET
ISP
LOCAL NETWORK
HOST
NETWORK LINK
COMM INT
CRT
MAIN MEMORY
MASS STORAGE
VIDEO AMP
VIDEO MEMORY
MOUSE
I/O
PROCESSOR
KEYBOARD
300
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326

FIG. 3

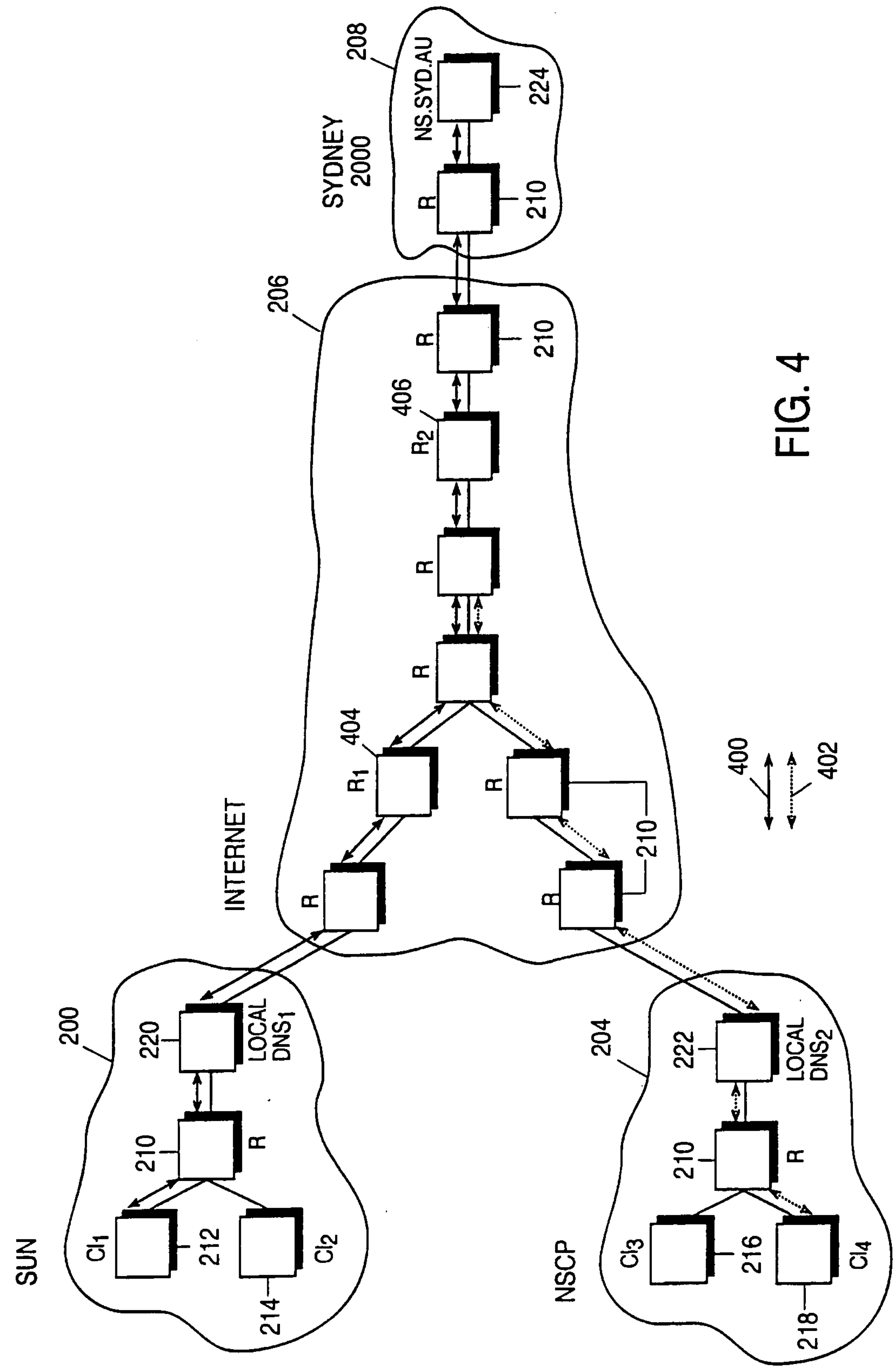

SYDNEY 2000
208
NS.SYD.AU
224
R
210
206
R
210
406
R_2
R
R
INTERNET
404
R_1
R
R
210
R
400
402
SUN
200
220
LOCAL DNS_1
210
R
Cl_1
212
Cl_2
214
NSCP
204
222
LOCAL DNS_2
210
R
Cl_3
216
Cl_4
218

FIG. 4

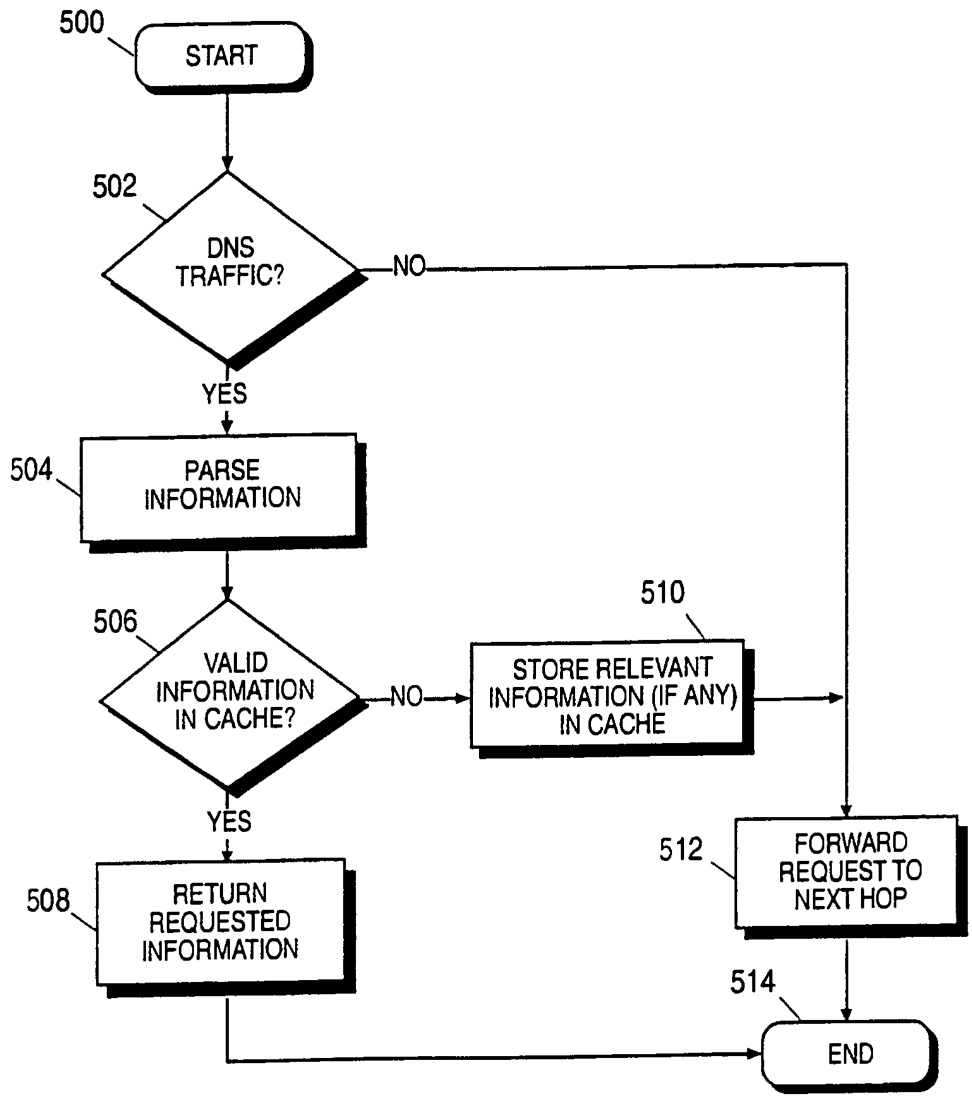

500
START
502
DNS TRAFFIC?
NO
YES
504
PARSE INFORMATION
506
VALID INFORMATION IN CACHE?
NO
510
STORE RELEVANT INFORMATION (IF ANY) IN CACHE
YES
508
RETURN REQUESTED INFORMATION
512
FORWARD REQUEST TO NEXT HOP
514
END

FIG. 5

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **11-167536**
(43)Date of publication of application : **22.06.1999**

(51)Int.Cl. G06F 13/00
G09C 1/00
H04L 12/46
H04L 12/28
H04L 12/66
H04L 12/56

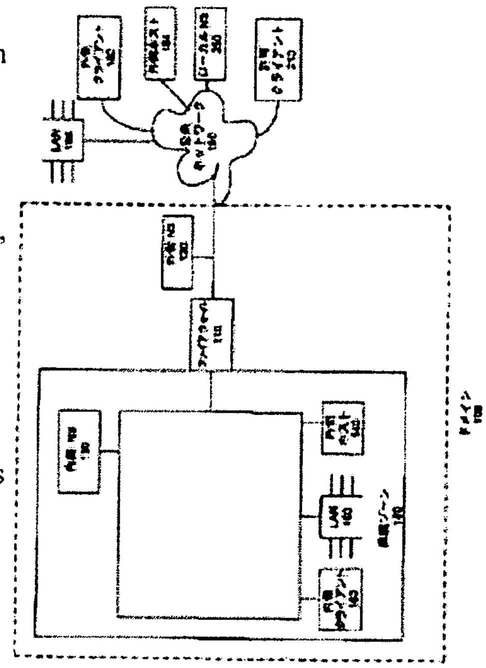
(21)Application number : **10-183088**
(22)Date of filing : **29.06.1998**

(71)Applicant : **SUN MICROSYST INC**
(72)Inventor : **AZIZ ASHAR**
MARKSON THOMAS

(30)Priority
Priority number : **97 883676** Priority date : **27.06.1997** Priority country : **US**

(54) **METHOD AND DEVICE FOR CLIENT/HOST COMMUNICATION USING COMPUTER NETWORK**

(57)Abstract:
PROBLEM TO BE SOLVED: To protect plural hosts on a private network wherein intermediate devices are placed behind an allowed client in a topology state by dynamically constituting the allowed client with the use of the address of a protection host and the keys and addresses of the intermediate devices (ciphering firewall, ciphering route, source gateway).
SOLUTION: A registered name server of a domain 100 is so constituted as to return a new resource address type (SX record) in response to a request for information needed for a secure communication with a protection host 140 placed in the domain 100. A resolver placed on (or related to) an allowed client 210 dynamically updates information used by the client to perform secure communication by using data in the SX record.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－167536

(43)公開日　平成11年(1999) 6月22日

(51)Int.Cl.⁶		識別記号	FI		
G06F	13/00	351	G06F	13/00	351Z
G09C	1/00	660	G09C	1/00	660E
H04L	12/46		H04L	11/00	310C
	12/28			11/20	B
	12/66				102D

審査請求　未請求　請求項の数70　ＯＬ　（全 27 頁）　最終頁に続く

(21)出願番号　特願平10－183088

(22)出願日　平成10年(1998) 6月29日

(31)優先権主張番号　08／883, 676

(32)優先日　1997年6月27日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　591064003
サン・マイクロシステムズ・インコーポレーテッド
SUN MICROSYSTEMS, INCORPORATED
アメリカ合衆国 94303 カリフォルニア州・パロ アルト・サン アントニオ ロード・901

(72)発明者　アシャー　アジズ
パキスタン　イスラマバード　エフ－10／4　ストリート　43　ハウス　143

(74)代理人　弁理士　谷　義一　（外3名）

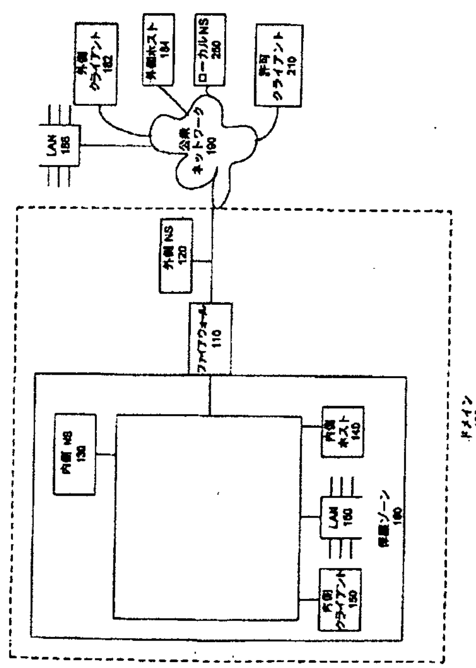
最終頁に続く

(54)【発明の名称】　コンピュータ・ネットワークを利用したクライアント／ホスト間の通信方法と装置

(57)【要約】

【課題】　保護ホストのアドレスおよび中間デバイス（暗号化ファイアウォール、暗号化ルータ、セキュア・ゲートウェイ）のキーとアドレスを使用して許可クライアントを動的に構成し、中間デバイスがその背後にトポロジ状に置かれている私用ネットワーク上の複数のホストを保護すること。

【解決手段】　ドメインの登録ネーム・サーバはそのドメインに置かれた保護ホストとのセキュア・コミュニケーションのために必要な情報の要求に応答して、新規のリソース・アドレス・タイプ（ＳＸレコード）を戻すように構成されている。許可クライアントに置かれている（さもなければ、それと関連づけられている）リゾルバはＳＸレコード内のデータを使用して、セキュア・コミュニケーションを処理するためにクライアントによって使用された情報を動的に更新する。



【特許請求の範囲】

【請求項1】　第1マシンによって使用される情報を動的に更新して前記第1マシンによる第2マシンへのセキュア・アクセスを容易化するための方法であって、

（a）前記第2マシンを収容しているドメインに関する照会を受信し、

（b）前記照会に応答するために必要な情報を要求するために前記ドメインの第1ネーム・サーバに連絡し、

（c）前記第1ネーム・サーバから第1応答を受信し、

（d）前記第2マシンに対応するセキュア・エクスチェンジャのＩＤを、前記第1応答の中のリソース・レコードから抜き出し、

（e）該第1マシンによって使用される第1データ構造を前記ＩＤを使用して更新して該第2マシンへのセキュア・アクセスを容易化するためのステップを含むことを特徴とする方法。

【請求項2】　請求項1に記載の方法において、前記照会を生成するアプリケーション・プログラムによって実行されることを特徴とする方法。

【請求項3】　請求項1に記載の方法において、前記第1データ構造を更新する前記ステップは前記マシンのアドレスを記録することを含むことを特徴とする方法。

【請求項4】　請求項1に記載の方法において、前記第1データ構造を更新する前記ステップは前記セキュア・エクスチェンジャの前記ＩＤを記録することを含むことを特徴とする方法。

【請求項5】　請求項1に記載の方法において、前記第1データ構造を更新する前記ステップは前記セキュア・エクスチェンジャの暗号データ項目を記録することを含むことを特徴とする方法。

【請求項6】　請求項5に記載の方法において、前記セキュア・エクスチェンジャの前記暗号データ項目は暗号キーであることを特徴とする方法。

【請求項7】　請求項5に記載の方法において、前記セキュア・エクスチェンジャの前記暗号データ項目はセキュアＤＮＳ　ＫＥＹリソース・レコードから取得されることを特徴とする方法。

【請求項8】　請求項5に記載の方法において、前記セキュア・エクスチェンジャの前記暗号データ項目は暗号アルゴリズムであることを特徴とする方法。

【請求項9】　請求項1に記載の方法において、前記第1データ構造を更新する前記ステップは前記セキュア・エクスチェンジャに関係するオリジナル・データベース名を記録することを含むことを特徴とする方法。

【請求項10】　請求項9に記載の方法において、前記オリジナル・データベース名は前記第1応答の中の前記リソース・レコードに対応するシグネーチャ・リソース・レコードからラベル・カウントを使用して導き出されることを特徴とする方法。

【請求項11】　請求項9に記載の方法において、前記オリジナル・データベース名は前記第1応答の中の前記リソース・レコードからの所有者名であることを特徴とする方法。

【請求項12】　請求項1に記載の方法において、前記第2マシンは前記照会のサブジェクトであることを特徴とする方法。

【請求項13】　請求項12に記載の方法において、前記照会を受信する前記ステップは前記第2マシンのアドレスの要求を受信することを含むことを特徴とする方法。

【請求項14】　請求項1に記載の方法において、前記第2マシンは前記ドメインに関係する第2ネーム・サーバであることを特徴とする方法。

【請求項15】　請求項1に記載の方法において、前記セキュア・エクスチェンジャの前記ＩＤは該セキュア・エクスチェンジャの名前であることを特徴とする方法。

【請求項16】　請求項15に記載の方法において、前記セキュア・エクスチャンジャの前記名前はＤＮＳ名であることを特徴とする方法。

【請求項17】　請求項1に記載の方法において、前記セキュア・エクスチェンジャの前記ＩＤは該セキュア・エクスチェンジャのアドレスであることを特徴とする方法。

【請求項18】　請求項1に記載の方法において、前記セキュア・エクスチェンジャは前記第2マシンを保護するファイアウォールであることを特徴とする方法。

【請求項19】　請求項1に記載の方法において、前記セキュア・エクスチェンジャは前記第2セキュア・マシンであることを特徴とする方法。

【請求項20】　請求項1に記載の方法において、前記第1データ構造はアクセス・コントロール・リストであることを特徴とする方法。

【請求項21】　請求項1に記載の方法において、前記第1データ構造はトンネル・マップであることを特徴とする方法。

【請求項22】　請求項1に記載の方法において、前記第1データ構造を更新する前記ステップは該第1データ構造内に少なくとも1つのデータ・セットを作成することを含むことを特徴とする方法。

【請求項23】　請求項22に記載の方法において、

（a）前記第1応答を受信する前記ステップは前記第2マシンのアドレスを該第1応答から抜き出すことを含み、そこでは該第2マシンは前記照会のサブジェクトとなっており、

（b）前記データ・セットを作成する前記ステップは、

（i）前記セキュア・エクスチェンジャの前記ＩＤを使用して、該セキュア・エクスチェンジャのパラメータを導き出し、

（ii）該セキュア・エクスチェンジャに関係するオリジナル・データベース名を導き出し、

（iii ）ａ）前記第２マシンの前記アドレス、ｂ）該セキュア・エクスチェンジャの前記パラメータ、およびｃ）前記オリジナル・データベース名を該データ・セットとしてストアすることを含むことを特徴とする方法。

【請求項２４】　請求項２３に記載の方法において、前記セキュア・エクスチェンジャの前記パラメータを導き出す前記ステップは前記第１応答から該パラメータを抜き出すことを含むことを特徴とする方法。

【請求項２５】　請求項２３に記載の方法において、前記セキュア・エクスチェンジャの前記パラメータを導き出す前記ステップは該パラメータに関して追加の照会を行うことを含むことを特徴とする方法。

【請求項２６】　請求項２３に記載の方法において、前記パラメータを導き出す前記ステップは該パラメータを前記ＩＤと等しいものと定義することを含むことを特徴とする方法。

【請求項２７】　請求項２３に記載の方法において、前記パラメータは前記セキュア・エクスチェンジャの暗号データ項目であることを特徴とする方法。

【請求項２８】　請求項２２に記載の方法において、

（ａ）前記第１応答を受信する前記ステップは前記ドメインに関係する第２ネーム・サーバのアドレスを導き出すことを含み、前記第２ネーム・サーバは該第１応答の中に指定されており、

（ｂ）前記データ・セットを作成する前記ステップは、

（ｉ）前記セキュア・エクスチェンジャの前記ＩＤを使用して、該セキュア・エクスチェンジャのパラメータを導き出し、

（ii）該セキュア・エクスチェンジャに関係するオリジナル・データベース名を導き出し、

（iii ）ａ）前記第２マシンの前記アドレス、ｂ）該セキュア・エクスチェンジャの前記パラメータ、およびｃ）前記オリジナル・データベース名を第１データ・セットとしてストアすることを含むことを特徴とする方法。

【請求項２９】　請求項２８に記載の方法において、前記第２ネーム・サーバの前記アドレスを導き出す前記ステップは前記第１応答から該アドレスを抜き出すことを含むことを特徴とする方法。

【請求項３０】　請求項２８に記載の方法において、前記第２ネーム・サーバの前記アドレスを導き出す前記ステップは該アドレスに関して追加の照会を行うことを含むことを特徴とする方法。

【請求項３１】　請求項２８に記載の方法において、前記セキュア・エクスチェンジャの前記パラメータを導き出す前記ステップは該パラメータを前記第１応答から抜き出すことを含むことを特徴とする方法。

【請求項３２】　請求項２８に記載の方法において、前記セキュア・エクスチェンジャの前記パラメータを導き出す前記ステップは該パラメータに関して追加の照会を行うことを含むことを特徴とする方法。

【請求項３３】　請求項２８に記載の方法において、前記第２マシンは前記ドメインに関係する前記第２ネーム・サーバであることを特徴とする方法。

【請求項３４】　請求項２８に記載の方法において、さらに、

（ａ）前記第１データ・セットを使用して、前記照会に対する第２応答を取得し、

（ｂ）前記第２マシンのアドレスを前記第２応答から抜き出し、

（ｃ）該第２マシンの名前に最良に合致する既存のオリジナル・データベース名を収めている既存のデータ・セットを前記第１データ構造から判断し、

（ｄ）前記既存のデータ・セットを使用して、（ｉ）該第２マシンの前記アドレス、（ii）前記セキュア・エクスチェンジャの既存のパラメータ、および（iii ）前記既存のオリジナル・データベース名を第２データ・セットにストアするステップを含むことを特徴とする方法。

【請求項３５】　請求項３４に記載の方法において、前記照会に対する前記第２応答を取得する前記ステップは、

（ａ）ネーム・サーバの応答性に関する情報を収めている第２データ構造を更新して、前記第２ネーム・サーバを次に照会するネーム・サーバとして含めておき、

（ｂ）前記第２データ構造を使用して、該照会をリダイレクトし、

（ｃ）該照会に対する第２応答を受信するステップを含むことを特徴とする方法。

【請求項３６】　請求項３５に記載の方法において、前記第２データ構造はＳＬＩＳＴであることを特徴とする方法。

【請求項３７】　請求項３４に記載の方法において、前記既存のデータ・セットを使用する前記ステップは該既存のデータ・セットからのデータ項目を指し示すことを含むことを特徴とする方法。

【請求項３８】　請求項３４に記載の方法において、前記既存のデータ・セットを使用する前記ステップは該既存のデータ・セットからデータ項目をコピーすることを含むことを特徴とする方法。

【請求項３９】　請求項２２に記載の方法において、前記データ・セットはａ）前記第２マシンのアドレスおよびｂ）前記セキュア・エクスチェンジャのパラメータを含むことを特徴とする方法。

【請求項４０】　請求項１に記載の方法において、前記ドメインの前記第１ネーム・サーバに連絡する前記ステップは前記照会を該第１ネーム・サーバに転送することを含むことを特徴とする方法。

【請求項４１】　請求項１に記載の方法において、前記ドメインの前記第１ネーム・サーバに連絡する前記ステップは前記セキュア・エクスチェンジャの前記ＩＤを要

求することを含むことを特徴とする方法。
【請求項42】　第1マシンによって使用される情報を動的に更新して、前記第1マシンによる第2マシンへのセキュア・アクセスを容易化するための方法であって、
（a）前記第2マシンのアドレスを取得し、
（b）該第2マシンへのセキュア・アクセスを容易化するために該第1マシンによって使用されるデータ構造を使用して、該第2マシンの名前に最良に合致する既存のオリジナル・データベース名を収めている既存のデータ・セットを前記データ構造から判断し、
（c）前記既存のデータ・セットを使用して、（i）該第2マシンの前記アドレス、（ii）セキュア・エクスチェンジャの既存のパラメータ、および（iii）前記既存のオリジナル・データベース名を第2データ・セットにストアするステップを含んでいることを特徴とする方法。
【請求項43】　請求項42に記載の方法において、前記既存のデータ・セットを使用する前記ステップは該既存のデータ・セットからのデータ項目を指し示すことを含むことを特徴とする方法。
【請求項44】　請求項42に記載の方法において、前記既存のデータ・セットを使用する前記ステップは該既存のデータ・セットからデータ項目をコピーすることを含むことを特徴とする方法。
【請求項45】　請求項42に記載の方法において、前記第2マシンの前記アドレスを取得する前記ステップは、
（a）前記アドレスの照会を受信し、
（b）前記照会を該第2マシンのドメインのネーム・サーバに転送し、
（c）前記ネーム・サーバから応答を受信し、
（d）前記応答から該アドレスを抜き出すステップを含むことを特徴とする方法。
【請求項46】　第1マシンによる第2マシンへのセキュア・アクセスを容易化するための方法であって、
（a）前記第2マシンを収容しているドメインに関係する前記第1マシンからの照会を第1ネーム・サーバで受信し、
（b）該第2マシンに対応するセキュア・エクスチェンジャのＩＤを取得し、
（c）前記ＩＤを含んでいる応答を生成し、
（d）該第1マシンのために前記応答を送信し、該応答は該第2マシンへのセキュア・アクセスを容易化するために該第1マシンによって使用可能であることを特徴とする方法。
【請求項47】　請求項46に記載の方法において、前記照会は前記第2マシンのアドレスの要求を含んでいることを特徴とする方法。
【請求項48】　請求項46に記載の方法において、前記応答は前記第2マシンへのセキュア・アクセスのために使用される情報を前記第1マシンが動的に更新することを可能にすることを特徴とする方法。
【請求項49】　請求項48に記載の方法において、前記ＩＤを取得する前記ステップは前記第2マシンに該当するデータベースから該ＩＤを取得することを含むことを特徴とする方法。
【請求項50】　請求項49に記載の方法において、前記応答を生成する前記ステップは、
（a）前記セキュア・エクスチェンジャのパラメータを取得し、
（b）前記パラメータを該応答に含めておくステップを含むことを特徴とする方法。
【請求項51】　請求項50に記載の方法において、前記セキュア・エクスチェンジャの前記パラメータは該セキュア・エクスチェンジャのアドレスを含むことを特徴とする方法。
【請求項52】　請求項50に記載の方法において、前記セキュア・エクスチェンジャの前記パラメータは該セキュア・エクスチェンジャの暗号データ項目を含むことを特徴とする方法。
【請求項53】　請求項52に記載の方法において、前記セキュア・エクスチェンジャの前記暗号データ項目は暗号キーであることを特徴とする方法。
【請求項54】　請求項52に記載の方法において、前記セキュア・エクスチェンジャの暗号データ項目は暗号アルゴリズムであることを特徴とする方法。
【請求項55】　請求項49に記載の方法において、前記セキュア・エクスチェンジャは第3マシンであることを特徴とする方法。
【請求項56】　請求項55に記載の方法において、前記第3マシンは前記第2マシンを保護するファイアウォールであることを特徴とする方法。
【請求項57】　請求項49に記載の方法において、前記セキュア・エクスチェンジャは前記第2マシンであることを特徴とする方法。
【請求項58】　請求項49に記載の方法において、前記セキュア・エクスチェンジャの前記ＩＤは該セキュア・エクスチェンジャの名前であることを特徴とする方法。
【請求項59】　請求項49に記載の方法において、前記セキュア・エクスチェンジャの前記ＩＤは該セキュア・エクスチェンジャのアドレスであることを特徴とする方法。
【請求項60】　請求項49に記載の方法において、前記照会に対する返答は前記データベースに存在せず、前記応答を生成する前記ステップは、
（a）前記第2マシンを収容している前記ドメインに関係する第2ネーム・サーバのＩＤを取得し、
（b）前記第2ネーム・サーバの前記ＩＤを該応答に含めておくステップを含むことを特徴とする方法。

【請求項６１】　請求項６０に記載の方法において、前記応答を生成する前記ステップは前記第２ネーム・サーバのアドレスを前記応答に入れて提供することをさらに含むことを特徴とする方法。

【請求項６２】　請求項４９に記載の方法において、前記照会に対す返答は前記データベースに存在し、前記応答を生成する前記ステップは

（ａ）該照会に対する前記返答を取得し、

（ｂ）該照会に対する該返答を該応答に含めておくステップを含むことを特徴とする方法。

【請求項６３】　第１マシンによる第２マシンへのセキュア・アクセスを容易化するためのシステムであって、

（ａ）前記第２マシンを収容しているドメインに関する照会を受信するように構成された制御ロジックと、

（ｂ）前記ドメインの第１ネーム・サーバに連絡して、前記照会に応答するために必要な情報を要求するように構成された制御ロジックと、

（ｃ）前記第１ネーム・サーバから第１応答を受信するように構成された制御ロジックと、

（ｄ）該第２マシンに対応するセキュア・エクスチェンジャのＩＤを、前記第１応答の中のリソース・レコードから抜き出すように構成された制御ロジックと、

（ｅ）該第２マシンへのセキュア・アクセスを容易化するために前記第１マシンによって使用される第１データ構造を前記ＩＤを使用して更新するように構成された制御ロジックであって、前記第１データ構造は該第２マシンに対応するデータ・セットを含んでいるものとを備えていることを特徴とするシステム。

【請求項６４】　請求項６３に記載のシステムにおいて、前記照会を生成するように、および前記生成された照会を該照会を受信する前記ロジックに与えるように構成されたソフトウェア・アプリケーション・プログラム内に具現化されていることを特徴とするシステム。

【請求項６５】　第１マシンによる第２マシンへのセキュア・アクセスを容易化するためのデータ構造を含んでいるコンピュータ可読媒体であって、前記データ構造は、

（ａ）前記第２マシンのアドレス、

（ｂ）該第２マシンに対応するセキュア・エクスチェンジャのパラメータ、および

（ｃ）前記セキュア・エクスチェンジャに関係するオリジナル・データベース名をもつトンネル・マップを含んでいることを特徴とするコンピュータ可読媒体。

【請求項６６】　請求項６５に記載のコンピュータ可読データ構造において、前記オリジナル・データベース名は前記セキュア・エクスチェンジャを示すリソース・レコードに対応するシグネーチャ・リソース・レコードからラベル・カウントを使用して導き出されることを特徴とするコンピュータ可読データ構造。

【請求項６７】　請求項６５に記載のコンピュータ可読データ構造において、前記オリジナル・データベース名は前記セキュア・エクスチェンジャを示すリソース・レコードからの所有者名であることを特徴とするコンピュータ可読データ構造。

【請求項６８】　請求項６５に記載のコンピュータ可読データ構造において、前記第１マシンに関連づけられたリゾルバ・プログラムによって生成されることを特徴とするコンピュータ可読データ構造。

【請求項６９】　第１マシンによる第２マシンへのセキュア・アクセスを容易化するためのソフトウェア・プログラムを具現化しているコンピュータ可読媒体であって、前記ソフトウェア・プログラムは、

（ａ）前記第２マシンを収容しているドメインに関する照会を受信するように構成されたプログラム・コードと、

（ｂ）前記ドメインの第１ネーム・サーバに連絡して、前記照会に応答するために必要な情報を要求するように構成されたプログラム・コードと、

（ｃ）前記第１ネーム・サーバから第１応答を受信するように構成されたプログラム・コードと、

（ｄ）該第２マシンに対応するセキュア・エクスチェンジャのＩＤを、前記第１応答の中のリソース・レコードから抜き出すように構成されたプログラム・コードと、

（ｅ）該第２マシンへのセキュア・アクセスを容易化するために前記第１マシンによって使用される第１データ構造を前記ＩＤを使用して更新するように構成されたプログラム・コードであって、前記第１データ構造は該第２マシンに対応するデータ・セットを含んでいるものとを備えていることを特徴とするコンピュータ可読媒体。

【請求項７０】　搬送波に具現化されていて、第１マシンによる第２マシンへのセキュア・アクセスを容易化するためのコンピュータ・データ信号であって、該データ信号は、

（ａ）前記第２マシンを収容しているドメインに関する照会を受信するように構成されたコード・セグメントと

（ｂ）前記ドメインの第１ネーム・サーバに連絡して、前記照会に応答するために必要な情報を要求するように構成されたコード・セグメントと、

（ｃ）前記第１ネーム・サーバから第１応答を受信するように構成されたコード・セグメントと、

（ｄ）該第２マシンに対応するセキュア・エクスチェンジャのＩＤを、前記第１応答の中のリソース・レコードから抜き出すように構成されたコード・セグメントと、

（ｅ）該第２マシンへのセキュア・アクセスを容易化するために前記第１マシンによって使用される第１データ構造を前記ＩＤを使用して更新するように構成されたコード・セグメントであって、前記第１データ構造は該第２マシンに対応するデータ・セットを含んでいるものとを含んでいることを特徴とするコンピュータ・データ信号。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は一般的にはコンピュータ・ネットワークに関し、具体的には、コンピュータ・ネットワークを利用する許可(authorized)クライアントと保護ホスト間のセキュア・コミュニケーションに関する。

【0002】

【従来の技術】A　ネットワーク・アドレス

コンピュータは相互に接続されてネットワークを形成し、これらのネットワークは他のネットワークに接続されてインターネットを形成している。「Internet（インターネット）」と呼ばれる世界的規模のインターネットの利用は、会議室(down the hall）にだけではなく、海外に置かれたホスト・コンピュータと通信する必要のあるクライアント・マシン上でプログラムを実行させる人が増加するのに伴って急激に増加している。Internet上の各ホストはwww.whitehouse.govといった固有の名前、および128．102．252．1．といった対応するネットワーク・アドレスをもっている。US Postal Service （米国郵便サービス）を通してレターを郵送する人が受取人の住所を知っている必要があるのと同じように、ネットワークを通してホストと通信するクライアントはホストのネットワーク・アドレスを知っている必要がある。しかし、通常は、クライアントはホストの名前だけを知っている。

【0003】Internetの世界では、ホストの名前とアドレスは世界の各国に置かれているコンピュータ上のデータベースにストアされている。これらのデータベースの1つをもち、ホスト・アドレスの照会(queries）に応答するコンピュータは、「ドメイン・ネーム・サーバ(Domain Name Server)」または単純に「ネーム・サーバ」を含めて、種々の名前で知らされている。非常に多数のホスト・コンピュータはInternetアドレスをもっているので、すべてのホストの名前とアドレス情報を1つのデータベースに保存しておくことは実用的でない。その代わりに、このような情報は世界各国のInternetドメイン・ネーム・サーバ間に分散されている。

【0004】ドメイン・ネーム・サーバおよびそれらに関連づけられた名前とアドレス・データベースは、アドレス照会に応答するために使用される1つのシステムにすぎない（「リゾルビングアドレス(resolving addresses）」とも呼ばれる）。「ディレクトリ・サービス」、「ディレクトリ・システム」、「DS」といった用語やその他の用語は、一般に、オンライン・データベースから情報を取り出してネットワーク経由で照会に応答するシステムを指すために使用されている。例えば、X500ディレクトリ・システム標準に準拠して実現されている分散データベースには、ネットワーク・アドレス以外にも、他の多数の種類の情報（例えば、人の名前とアドレス、プリンタの名前とロケーション、電話番号とファックス番号）を含めることが可能になっている。X500の詳細は当業者には周知であるので、ここで詳細に説明することは省略する。参考文献としては、例えば、Uyless D. Black 著「OSI：A Model for Computer Communication Standards（OSI：コンピュータ通信標準モデル）」、Prentice-Hall （1991），pp．388－89がある。

【0005】ある企業がInternetに接続するときは、その企業はそのドメイン名（例えば、sun.com)を登録する。これは第2レベル・ドメインと呼ばれている。企業は第2レベル・ドメインのすべてのアドレス照会がInternetドメイン・ネーム・システムによって送られる先の公開ネーム・サーバを少なくとも2つ指名し、登録しなければならない。これらのサーバは、以下では、ドメインの「登録」ネーム・サーバと呼ぶことにする。企業はそのドメインをもっと小さなセグメントに分割することがよくあり、これらのセグメントは「ゾーン」と呼ばれている（例えば、eng.sun.com およびcorp.sun.com）。当業者ならば理解されるように、「ゾーン」という用語はドメインを任意に分割したものを指す場合があり、この中にはドメイン全体自体も含まれる。企業はそれぞれのゾーンだけで「権限をもつ」ネーム・サーバを指名することができる。この場合、各ゾーンは独自のデータベース（「ゾーン・データベース」）をもち、そこには、そのゾーンに置かれているマシンの名前、アドレス、およびその他の情報が収容されている。説明の便宜上、「ネーム・サーバ」という用語は、以下では、サーバのデータベース（例えば、ドメイン・ネーム・サーバまたはディレクトリ・サーバ）内の情報の照会に応答するサーバを意味するために使用され、「ゾーン・データベース」という用語は、それが第2レベル・ドメインを包含するか、もっと小さなゾーンを包含するかに関係なく、そのデータベースを意味するために使用されている。当業者ならば理解されるように、「データベース」という用語は編成された情報の集まり一切を意味することができる。

【0006】企業があるゾーン内のマシンのアドレスを公開して、見えるようにすることを選択していれば、そのゾーンを収めている第2レベル・ドメインの登録ネーム・サーバはそのゾーン内のマシンのアドレス照会を権限をもつゾーン・ネーム・サーバに送るように構成されている。しかし、企業がゾーンのネットワーク・トポロジを隠す必要があるときは、登録ネーム・サーバはゾーン・ネーム・サーバに関するどの情報ももたないように構成され、そのゾーン内のマシンだけが照会をゾーン・ネーム・サーバに送るように構成されている。このような可視制限ゾーン(visibility-limited zone）は「保護ゾーン」と呼ぶことができ、そこに置かれたマシンは「保護マシン(protected machines)」と呼ぶことができ

る。従って、マシンのアドレスが公開されて、見えるようにされたかどうかは、ネットワーク上で稼働しているプログラム相互間のやりとり(interaction) に影響することになる。

【0007】上述したように、クライアント上で実行されているアプリケーション・プログラムが別のロケーションに置かれたホストに連絡する必要があるときは、そのアプリケーションはそのホストのアドレスを必要とする。一般に、アプリケーション・プログラムは照会を「リゾルバ(resolver)」プログラム（これもクライアント上で実行されている）に送って、アドレスを要求することがある。リゾルバ・プログラムはローカル・ファイルをチェックし、ホスト・アドレスを要求するためのデフォルト・ネーム・サーバが分かると、その照会をデフォルト・ネーム・サーバに渡すことになる。説明の便宜上、このデフォルト・ネーム・サーバは、以下ではクライアントの「ローカルＮＳ」と呼ぶことにする。ローカルＮＳは要求されたアドレスをすでにもっている場合もあれば、そのアドレスをもつサーバ（例えば、第２レベル・ドメインの登録ネーム・サーバまたはゾーンの権限をもつネーム・サーバ）に到達するまで、必要に応じて他のネーム・サーバに連絡していく場合もある。ローカルＮＳが照会に対する応答を受信すると、ローカルＮＳはその応答をリゾルバに戻し、リゾルバは応答を処理し、アドレスをクライアントに引き渡す。Internetドメイン・ネーム・システムおよびリゾルバの上記説明とその他の詳細は当業者には周知であるので、ここでは詳しく説明することは省略する。参考文献としては、例えば、Sidnie Feit 著「ＴＣＰ／ＩＰ」、McGraw-Hill（１９９７）があり、第１２章に詳しく説明されている。

【0008】Ｂ　許可クライアント

現在のテクノロジは、ネットワークを利用したコミュニケーションをいくつかの側面から見たとき、十分に解決していない側面がいくつかある。企業のネットワーク・ポリシを実現するためには、上述したように、ネットワーク管理者は、保護マシンのアドレスを他の保護マシンだけに見えるようにすることによってネットワーク・トポロジを隠すようにゾーンをセットアップすることができる。しかし、ネットワーク管理者は保護ゾーンの外にいる許可クライアントが、保護ゾーンの内側にいるホストと通信できるようにしたい場合もある。ネットワーク管理者は許可クライアントが通信できる保護ホストのアドレスを、そのクライアント上の１つまたは２つ以上の静的構成ファイルにストアしておくこともできる。その場合には、これらの構成ファイルは保護ホストのアドレスが変更されるたびに、すべての許可クライアント側で更新する必要がある。ネットワーク管理者は置換ファイルをすべての許可クライアントに送ることができるが、別の方法として、ネットワーク管理者は変更された情報を、許可クライアントへのアクセス権をもつ人に配布して「手操作（マニュアル）」で入力させることもできる。このような人は構成ファイルを直接に編集することも、プログラム（例えば、コマンドライン・プログラムまたはグラフィカル・ユーザ・インタフェース）を使用して変更情報を入力することもできる。

【0009】クライアントの数と移動性が増加するに伴い、これらの構成ファイルを最新に保つことは、不可能ではないにしても、煩わしい作業である。ネットワーク管理者は保護ホストのアドレスを使用して許可クライアントを構成し、人間の介入なしですべての許可クライアント上の構成ファイルを変更できるようにする方法を必要としている。本発明の種々実施例が提供する解決方法によれば、許可クライアントは中央ロケーションにストアされ、維持されている情報を使用して各自のファイルを動的に更新することができる。その場合、ネットワーク管理者はすべての許可クライアント上のファイルを更新しなくても、容易にアクセス可能なロケーションに置かれている情報を更新するだけですむことになる。

【0010】Ｃ　セキュア・コミュニケーション

許可クライアントはコミュニケーションを確立するために、保護ホストのアドレス以上のものを必要とすることがよくある。このようなことは、クライアントとホストがコミュニケーションが「セキュア（安全保護）」であるかを確かめたいときに起こっている。セキュア・コミュニケーションには、プライバシ、保全性、および認証という問題が含まれている。ここでプライバシとは、あるクライアントがネットワークを利用して機密情報を送信するとき、意図するホストだけがそれを読み取り、理解できることを意味する。保全性(integrity) とは、送信中にだれもがメッセージを変更しなかったことを意味する。認証(authentification)とは、そのメッセージがメッセージが要求するクライアントからのものであることがホストに保証されることを意味する。標準的暗号手法としては、ＤＥＳやＲＳＡなどのアルゴリズム、およびディジタル・シグネーチャ、ディジタル証明、ＳＫＩＰなどの、他のテクノロジやプロトコルがある。必要に応じて、これらの暗号手法（または同等のセキュリティ手法）は種々側面から見たプライバシ、保全性、および認証を保証するために使用されているのが普通である。

【0011】保護ホストのアドレスを許可クライアントに提供するのと同じように、セキュア・コミュニケーションはネットワークを利用したコミュニケーションの１つの側面であり、この側面も現在のテクノロジでは十分に解決されていない。ある種のネットワーク構成では、ネットワーク・セキュリティ・システムであるファイアウォール(firewall)が保護マシンへのアクセスを管理している。許可クライアントが保護マシンと機密に通信できるようにするためには、ファイアウォールはそのクライアントからのコミュニケーションがファイアウォール

を経由するように構成されていなければならない。さらに、保護ホストとセキュア・コミュニケーションを行うためには、ホストのアドレスのほかに、許可クライアントは追加の情報を必要とする。この追加情報としては、（１）保護ホストのために暗号化を行うファイアウォールのアドレスとキー、および（２）使用される暗号アルゴリズム（および他の必要な暗号手法）がある。

【００１２】許可クライアントがこの追加情報を取得すると、その追加情報はホスト・アドレスと一緒に、暗号化オペレーションを処理するクライアントのコンポーネント（例えば、アプリケーション・プログラム、オペレーティング・システム、またはハードウェアの暗号プロセッサ）によって使用されるデータ構造にストアされるのが一般である。例えば、ＳＫＩＰテクノロジでは、このような「アウトバウンド・セキュア・メッセージ」はインバウンド・アクセス情報と一緒に、クライアントのアクセス・コントロール・リストにストアされている。しかし、当業者ならば理解されるように、アウトバウンド・メッセージ情報は適切なデータ構造であれば、どのデータ構造にもストアすることが可能である。

【００１３】アウトバウンド・セキュア・メッセージ情報を収めているデータ構造はホストのアドレスまたは暗号情報が変更されるたびに、すべての許可クライアント側で更新する必要がある。この場合も、本発明の種々の実施例によれば、許可クライアントは中央ロケーションにストアされ、維持されている情報を使用して各自のデータ構造を動的に更新することができる。説明の便宜上、「許可クライアント」という用語は、ここでは、本発明を使用するように構成され、許可クライアントが通信する保護ホストのファイアウォールを経由してコミュニケーションが許されているクライアントを意味するものとして用いられている。

【００１４】

【発明の要約】本発明によれば、保護ホストのアドレスおよび中間デバイス（例えば、暗号化ファイアウォール、暗号化ルータ、セキュア・ゲートウェイ）のキーとアドレスを使用して許可クライアントを動的に構成し、その中間デバイスがその中間デバイスの背後にトポロジ状に置かれている私用(private) ネットワーク上の複数のホストを保護するようした方法および装置が提供されている。ドメインの登録ネーム・サーバはそのドメインに置かれた保護ホストとのセキュア・コミュニケーションに必要な情報の要求に応答して、新規のリソース・レコード・タイプ（ここでは、ＳＸレコードと名づけている）を戻すように構成されている。許可クライアントに置かれた（さもなければ、それと関連づけられた）リゾルバ（ｒｅｓｏｌｖｅｒ）はＳＸレコード内のデータを使用して、セキュア・コミュニケーションを処理するためにクライアントによって使用される情報を動的に更新するように構成されている。

【００１５】本発明のいくつかの実施例を使用すると、多数の利点が得られる。そのような利点としては、保護ホストのアドレスを使用してクライアントを動的に構成するシステム、保護ホストとのセキュア・コミュニケーションのためにクライアントを動的に構成するシステム、およびネットワーク管理者がセキュア・コミュニケーションのために必要なアドレスと暗号情報を中央で管理できるようにするシステムがあるが、本発明はこれらに限定されるものではない。本発明のいくつかの実施例の上記利点およびその他の利点は、下述する詳細な説明の中で明らかにする。

【００１６】

【発明の実施形態】以下、本発明の１つまたはいくつかの実施例の理解を容易にするために、添付図面を参照して本発明について詳しく説明する。

【００１７】ネットワークは種々構成が可能であり、その構成はローカル・エリア・ネットワーク（ＬＡＮ）、広域ネットワーク（ＷＡＮ）、イントラネット、インターネット、およびInternetといったように、多彩な名前が付けられている。代表的なインターネット構成は私用ＬＡＮおよび公衆(public)Internetの一部を含む、任意の数のネットワークで構成されている。任意の数のコンピュータをこれらのネットワークに接続することができる。これらのコンピュータは様々な機能に利用することができが、特定の機能を反映する用語で表されることがよくある。１つの例では、ある人は別のコンピュータと通信する必要のあるパーソナル・コンピュータ（ＰＣ）上でプログラムを実行している。この場合のＰＣはクライアントと呼ばれ、他方のコンピュータはサーバまたはホストと呼ばれている。別の例では、２つのネットワークを接続するコンピュータはゲートウェイと呼ばれている。これらの例におけるコンピュータはいずれも、単純にマシンと呼ばれることもある。当業者ならば理解されるように、本発明はネットワークおよびそこに接続されたコンピュータのどちらの場合も、特定の構成を要求するものではない。従って、以下では、ある特定の構成（インターネットを利用したクライアントとホスト間のコミュニケーション）を参照して本発明を説明しているが、以下の説明は任意のネットワーク・タイプ上で動作する、どのコンピュータにも適用されることはもちろんである。

【００１８】Ａ　本発明が実施される環境

図１は、本発明の実施例を実施できる代表的なインターネット構成を示したものである。この構成には、ファイアウォール１１０によって公衆(public)ネットワーク１９０に接続されているドメイン１００（例えば、sun.com ）が含まれている。ドメイン１００は保護ゾーン１８０（「ファイアウォールの内側」と呼ばれることもある）を含み、保護ゾーンは任意の数のマシンを任意の構成で含むことができる。この例では、内側ホスト１４

0、LAN160、内側クライアント150、および内側NS130はすべて保護ゾーン180に置かれている。外側NS120はドメイン100の登録ネーム・サーバであり、内側NS130は保護ゾーン180の権限をもつネーム・サーバである。

【0019】ほとんど無制限の数のマシンとネットワークが公衆ネットワーク190に接続されている。図1に示すように、代表的な構成には、外側クライアント182、外側ホスト184、LAN186、ローカルNS250、および許可クライアント210が含まれている。図2、図3および図4を参照して以下で明らかにするように、代表的な許可クライアント210には、アプリケーション215、そのローカルNS250を示している構成ファイル220、リゾルバ225、暗号プロセッサ230、オペレーティング・システム235、およびトンネル・マップ500が含まれている（詳細は後述する）。代表例として、これらのコンポーネントは許可クライアント210側の1つまたは2つ以上のコンピュータ可読媒体またはメモリに置かれている。

【0020】B 問題

上述したシステム・アーキテクチャが与えられているとき、許可クライアント210で実行されているアプリケーション210が保護ゾーン180内の保護ホスト140と機密に通信する必要が起こったとき、どのようなことが行われるか。アプリケーション215がそれを行うためには、その前に、アウトバウンド・セキュア・メッセージ情報が必要になる。この情報は許可クライアント210にストアされており、情報としては、内側ホスト140のアドレス、ファイアウォール110のアドレスとキー、および使用される暗号プロトコルがある。クライアントの数と移動性が増加するに伴い、人間の介入に頼ってアウトバウンド・セキュア・メッセージ情報を最新に保つことは煩雑な作業であり、あるいは不可能である。本発明の種々実施例によれば、この問題は許可クライアントが中央ロケーションにストアされ、維持されている情報を使用して、各自のアウトバウンド・セキュア・メッセージ情報を動的に更新できるようにすることによって解決されている。以下のセクションでは、クライアントとネーム・サーバ間のメッセージの構造と内容、仲介の働きをするリゾルバ・プログラム、およびシステムがどのように構成されているか、について詳しく説明する。

【0021】C. ネーム・サーバ・メッセージおよびリソース・レコード

ネーム・サーバ・メッセージはヘッダと4つのセクション（1）照会(query)、（2）返答(answer)、（3）権限(authority)、（4）追加(additional)から構成されている。返答、権限、および追加セクションは、ネーム・サーバが照会に応答して送信するリソース・レコードを収めている。リソース・レコード・タイプは多数存在し、各々はそのレコード・タイプのデータを収めているデータ・フィールドを含んでいる。例えば、要求されたホストのアドレスはAレコードのデータ・フィールドに入って戻され、権限をもつネーム・サーバの名前はNSレコードのデータ・フィールドに入って戻される。

【0022】セキュア・コミュニケーションの必要性をサポートするために、Internetドメイン・ネーム・システム（「セキュアDNS」）のあるバージョンはKEYとSIGリソース・レコード・タイプを含む、セキュリティ拡張機能(extensions)を使用している。KEYリソース・レコードは公開キーと関連情報を配布するために使用できる。つまり、KEYレコードはキー、キー名、またはアルゴリズムを収めることができる。SIG、つまり、「シグネーチャ」リソース・レコードは他のリソース・レコードに入っているデータを認証するために使用できる。SIGレコードのデータ・フィールドの1つは「ラベル(labels)」フィールドである。このフィールドは、オリジナルSIGレコード所有者名がゾーン・データベースに置かれているときラベルがいくつあるかをカウントしたものである（例えば、*.sun.comが2つのラベルをもっているのは、ルートを表すヌル・ラベル（“.”）とワイルドカード（“*”）はカウントに含まれないためである）。従って、このラベル・カウントはワイルドカード置換の結果としてリトリーブされたレコードのオリジナル名を導き出すために使用される（詳細は後述する）。このオリジナル名は、例えば、ディジタル・シグネーチャを検証するために必要になる。

【0023】本発明の一実施例では、セキュアDNSによって提供されるKEYとSIGリソース・レコードを使用している。セキュアDNSの詳細は当業者には周知であるので、ここでは、これ以上詳しく説明することは省略する。参考文献としては、例えば、RFC 2065－「Domain Name System-Security Extensions（ドメイン・ネーム・システム－セキュリティ拡張機能」（1997）がある。当業者ならば理解されるように、本発明の一実施例では、セキュアDNS機能を利用しているが（例えば、レコードのオリジナル名を導き出し、シグネーチャを検証するために）、すべての実施例がこの機能を必要とするとは限らない（つまり、これらは十分な能力をもつ他のシステムを使用して実現することが可能である）。

【0024】D SXレコード

セキュリティ拡張機能で上に示したように、Internetドメイン・ネーム・システムはユーザが新規のリソース・レコード・タイプを自由に作成できる点でオープンエンド(open-ended)になっている。本発明の種々実施例によれば、さらに、SXレコードと名づけた別の新規レコード・タイプが追加されている。SXレコードのデータ・フィールドは、そのレコードの所有者に関連する「セキュア・エクスチェンジャ(secure exchanger)」のID

（例えば、名前またはアドレス）を収めている。セキュア・エクスチェンジャはセキュア・コミュニケーションを自身のために、または別のマシンのために処理するマシンである（例えば、暗号化または解読を実行する）。この機能を実行するために、セキュア・エクスチェンジャは暗号データ（例えば、キーまたはアルゴリズム）を使用する。セキュア・エクスチェンジャのＩＤと暗号データはセキュア・エクスチェンジャのパラメータと総称することができる。ファイアウォールはセキュア・エクスチェンジャ機能を頻繁に実行するので、「ファイアウォール１１０」という用語は、ここでは、セキュア・エクスチェンジャを意味するために用いられている。当業者ならば理解されるように、該当の暗号化機能を持つマシンならば、どのマシンでもセキュア・エクスチェンジャとして機能させることができる。

【００２５】また、当業者ならば理解されるように、「ＳＸ」は任意のレコード・タイプＩＤであり、ＳＸレコード・タイプが定義されていれば、クライアントは明示的にそのタイプのレコードをネーム・サーバに要求することができる。別の方法として、ネーム・サーバは他のレコードの照会に対する返答を含む応答に入れてＳＸレコードを戻すように構成することも可能である。例えば、クライアントがホスト・アドレスについて照会すると、ネーム・サーバはホスト・アドレスを応答セクションに、ＳＸレコードを追加セクションに入れて応答を送信することになる。本発明の他の実施例には、ＳＸレコードを追加または権限セクションに入れて戻し、応答の返答セクションは空のままにしておくようにネーム・サーバの振舞をカストマイズすることを含めることも可能である。言い換えれば、応答は未要求のリソース・レコードだけを含むことになる。上述した説明から明らかなように、当業者ならば理解されるように、本発明はＳＸレコードが応答のどの特定セクションに入って送られるかには左右されない。ＳＸレコード内のデータは、保護ホストとのセキュア・コミュニケーションのためにクライアントによって使用された情報を更新するために、リゾルバと呼ばれるプログラムによって使用される。

【００２６】Ｅ　リゾルバの概要

リゾルバは、ネーム・サーバと、クライアント上で実行されているアプリケーション・プログラムとの間の仲介役をするプログラムである。リゾルバは情報の照会をアプリケーション・プログラムから受信し、その照会を該当のネーム・サーバに送信し、もしあれば、応答を要求側アプリケーションに戻す。照会のタイプとしては、所与のホスト名のホスト・アドレス、所与のホスト・アドレスのホスト名、およびネーム・サーバ・データベースにストアされている情報の全体的ルックアップがある。リゾルバは一般的に照会の処理を次の４ステップで行う。（１）照会に対する返答がローカルにあれば、その返答を戻し、返答がなければ（２）返答を要求する最良のサーバを見つけ、（３）いずれかが応答するまでそのサーバに照会を送信し、（４）返答を処理する。

【００２７】ステップ（２）で照会するのに最良のサーバを見つけるために、リゾルバはサーバ名とゾーンのリストを、ＳＬＩＳＴと名づけた構造に保存している。ＳＬＩＳＴはデフォルト・サーバで初期化される。そのあとで、リゾルバはサーバとやりとりするたびに、リゾルバはどのサーバが必要とする情報をもっているかのリゾルバの「最良の推量(best guess)」でＳＬＩＳＴを更新する。この「最良の推量」は所与のマシンに関する照会に対する各サーバの応答性がどの程度であるか（例えば、応答時間またはサーバが応答した頻度）に基づいて行われることがよくある。従って、過去の実績に基づく応答性は将来の照会用にＳＬＩＳＴを最適化するために使用されている。当業者ならば理解されるように、リゾルバはこの基準または他の基準に従ってＳＬＩＳＴを維持するようにプログラムすることが可能である。

【００２８】上述した説明は、リゾルバが実行する機能、およびその機能の実現方法を高度にカストマイズできることを示す一例である。リゾルバのこれらの説明および他の詳細は当業者には周知であるので、ここで詳しく説明することは省略する。参考文献としては、例えば、ＲＦＣ１０３４－「Domain Names-Concepts and Facilities（ドメイン名－概念と機能）」（１９８７）およびＲＦＣ１０３５－「Domain Names-Implementation and Specification （ドメイン名－実現方法と仕様）」（１９８７）がある。

【００２９】Ｆ　リゾルバの機能

本発明の種々実施例は、保護ホストとのセキュア・コミュニケーションのために使用される情報（つまり、アウトバウンド・セキュア・メッセージ情報）を収めている、クライアント側のデータ構造を動的に更新するようにリゾルバ機能をカストマイズすることによって実現されている。このようなデータ構造はデータ・セットから構成され、そのフィールドは「トンネル情報」（例えば、デスティネーションとセキュア・エクスチェンジャ・アドレス）と関連暗号データ（例えば、セキュア・エクスチェンジャのキーまたはアルゴリズム）を収めているのが代表的である。ここで、「トンネル・マップ」という用語はそのようなデータ構造を意味するために用いられ、「トンネル・マップ・エントリ」という用語はデータ・セットの１つを意味するために用いられている。

【００３０】本発明の一実施例によれば、トンネル・マップ・エントリはネーム・サーバ・メッセージからのＳＸレコードに入っているセキュア・エクスチェンジャのカバレッジ有効範囲(scope of coverage) を示すフィールドも含んでいるが、このフィールドは現在この分野では使用されていないものである。言い換えれば、この新規フィールドはエントリ内のセキュア・エクスチェンジャが暗号化メッセージを、どのマシンに「トンネルから

通過」させるかを示している。詳細は後述するが、このフィールドを使用すると、既存のものから新規のトンネル・マップ・エントリを作成できるので、エントリ作成プロセスを効率化することができる。しかし、本発明のすべての実施例がこのフィールドを必要とするとは限らないので、これはトンネル・マップ・エントリから省くことも可能である。このような実施例の１つは「その他の実施例」のセクションに示されている。

【００３１】図９はフィールド４　５４０を含むトンネル・マップ・エントリ５００を示す概略図である。図９に示すように、行(row) １はエントリのフィールドの内容を概略記述し、行２と行３－４は本発明の２実施例の場合のフィールド・データを具体的に記述している。トンネル・マップ・エントリ５００がどのように作成され、使用されるかの詳細は、「許可クライアントで実現される発明」のセクションの後で説明することにする。本発明の種々実施例では、トンネル・マップ情報はＩＰＳＥＣやＳＫＩＰなどの、標準トンネル・プロトコルと関連づけて使用されている。当業者ならば理解されるように、本発明はトンネル・マップ内の情報の内容またはロケーションに行った変更を容易に受け入れることができる。

【００３２】当業者には公知であるように、リソース・レコードは存続時間（time-to-live（ＴＴＬ））フィールドを含んでおり、これはレコードの情報がいつまで信頼できるかを示している。ＳＸレコード内のＴＴＬフィールドはそのレコードから導き出されたトンネル・マップ・エントリの寿命を判断するために使用できる。しかし、マシンのリブート時にトンネル・マップを再初期化するといった他の手法を用いて、トンエル・マップを最新に保つことも可能である。本発明はどの特定手法にも限定されないが、本発明によれば、これらの手法およびこの分野で公知の他の手法を用いてトンネル・マップの正確性を保つことが可能である。

【００３３】Ｇ　リゾルバのロケーション

リゾルバの機能をカストマイズできるだけではなく、その機能を１つまたは２つ以上のコンポーネントの中で実現することも可能である。リゾルバ２２５という用語は、ここでは、本発明によって提供される全機能を意味するために用いられており、かかる機能を実現するために使用されるコンポーネントの数またはそのコンポーネントが置かれるロケーションは無関係である。図２、図３および図４は許可クライアント２１０の構成例を示している。各構成において、許可クライアント２１０のアドレスは例えば１９９．２００．１．９に、そのローカルＮＳ２５０のアドレスは例えば１９９．２００．１．２になっている。従って、リゾルバ２２５によって使用される構成ファイル２２０は、ローカルＮＳ２５０のアドレスを収めている。アプリケーション２１５は許可クライアント２１０にインストールされている。暗号プロセッサ２３０が必要であれは、これも許可クライアント２１０にインストールされる。

【００３４】図２に示す構成では、リゾルバの全機能は１つのコンポーネントに実現されている。このケースでは、アプリケーション２１５はその照会をリゾルバ２２５に送付する。リゾルバ２２５は構成ファイル２２０からのローカルＮＳ２５０のアドレスを読み取り、照会をローカルＮＳ２５０に転送する。リゾルバ２２５は応答を受信すると、ここで説明したようにその応答を処理する。

【００３５】図３は、クライアントのリゾルバを変更することが望ましくないか、または可能でないとき実現できる構成を示したものである（例えば、クライアントではMicrosoft Windows が実行されている）。このケースでは、標準スタブ・リゾルバ２２６が許可クライアント自体へのループバックと共に使用される。リゾルバ２２５は許可クライアント２１０にインストールされているネーム・サーバ・ソフトウェアに組み込まれている。ループバックを実現するために、リゾルバ２２５は構成ファイル２２０を読み取り、ローカルＮＳ２５０のアドレスを許可クライアント２１０のアドレスで置き換える。リゾルバ２２５はローカルＮＳ２５０のアドレスを自身で使用するために保存しておく。このケースでは、アプリケーション２１５はその照会をスタブ・リゾルバ２２６へ送付し、リゾルバ２２６は変更された構成ファイル２２０を読み取り、照会をリゾルバ２２５へ送る。リゾルバ２２５は照会を受信すると、オリジナル構成ファイル２２０に残しておいたアドレスを使用して、その照会をオリジナル・ローカルＮＳであるローカルＮＳ２５０に転送する。なんらかの応答がリゾルバ２２５に戻されると、リゾルバ２２５はここで説明したように応答を処理する。

【００３６】図４に示す第３の構成では、アプリケーション２１５はリゾルバ２２５と一体になるように変更されている。従って、照会を行うには、アプリケーション２１５は構成ファイル２２０を読み取り、照会をローカルＮＳ２５０に送付する。変更されたアプリケーション２１５は応答を受信すると、それを処理する。当業者ならば理解されるように、本発明の精神と範囲から逸脱しない限り他の構成を使用することも可能である。

【００３７】Ｈ　システム・セットアップの概要

ＳＸレコードとリゾルバは上述したとおりであるが、その説明を前提として、このセクションではシステムの一実施例がどのようにセットアップされるかの概要を説明する。以下の概要では、図１がレファレンスとして使用され、「ネットワーク管理者」という用語はシステム・セットアップ・タスクのいずれかを実行する一切の個人を含むように広義に用いられている。これらの個人はネットワーク管理者とは別の名称をもっている場合がある（例えば、システム管理者、ＬＡＮ管理者、データベー

ス管理者、またはゾーン管理者）。実際には、エンドユーザおよびプログラマがこれらのタスクの一部を実行する場合もある。さらに、当業者ならば理解されるように、システム・セットアップ・タスクは一人の個人で実行されるとは限らない。システムをセットアップすることは、システムの3つの部分、つまり、（1）外側ＮＳ１２０である、ドメイン１００の登録ネーム・サーバ、（2）ファイアウォール１１０、および（3）許可クライアント２１０を構成することと見ることができる。

【００３８】外側ＮＳ１２０を構成するためにネットワーク管理者が実行するタスクとしては、ＳＸリソース・レコードを定義し、該当のレコードを外側ＮＳ１２０用のネーム・サーバ・データベースに追加することがある。この構成には、「登録ネーム・サーバで実現される発明」のセクションで詳しく説明されているように、外側ＮＳ１２０をカストマイズすることも含まれる。

【００３９】ファイアウォール１１０を構成することには、許可クライアント１２０と保護ゾーン１８０内側のマシン間の暗号化コミュニケーションを処理するようにファイルウォールをセットアップすることが含まれる。また、許可クライアント２１０からのコミュニケーションを認識し、許可するようにファイアウォール１１０２を構成することも含まれる。当業者に周知であって、これらの結果を達成できる手法ならば、どの手法でもファイアウォール１１０を構成するために使用することができる。

【００４０】本発明に従って動作するように許可クライアント２１０を構成するためには、次の２つの基本カテゴリに属するコンポーネントが必要である。第１のカテゴリには、リゾルバ２２５を実現するコンポーネントが含まれる。リゾルバ・コンポーネントの詳しい説明は「リゾルバのロケーション」のセクションに記載されている。第２のカテゴリには、許可クライアント２１０のために暗号オペレーションを実行するコンポーネント（以下では、暗号プロセッサ２３０と総称する）が含まれている。暗号オペレーションには、当業者ならば理解されるように、暗号化、解読、ハッシング(hashing)、ディジタル証明、ディジタル・シグネーチャ、その他がある。従って、暗号コンポーネントには、暗号化／解読ソフトウェアまたは暗号化機能を持つＰＣＭＣＩＡを含めることができるが、いかなる場合も、これらに限定されるものではない。

【００４１】Ｉ　登録ネーム・サーバで実現される発明
上述した概要セクションを背景として使用して、このセクションでは本発明の一実施例を実現する詳細について説明する。以下の説明では、留意すべき点が３つある。第一は、ネーム・サーバは任意のタイプのレコードを応答の特定のセクションに入れるのが代表的であるが、本発明によれば、そのような要件が必ずしも課されないことである。例えば、ＮＳレコードは権限セクションに入って送られるのが代表的であるが、本発明の実施例では、追加セクションが使用される。第二は、ネーム・サーバがリソース・レコードを応答に追加するとき、該当のＳＩＧとＫＥＹレコードも追加されることが暗黙になっていることである（つまり、各レコード・タイプとレコード所有者名の組み合わせごとに１つのＳＩＧレコード、およびＳＩＧレコードを生成するために使用されるＫＥＹレコード）。さらに、ＳＩＧとＫＥＹレコードは受信時に署名済みレコードを検証するために使用されることが暗黙になっている。第三は、レコードを応答に追加する実行ステップがオプションとして記述されているときは、これらのレコードは追加の照会を行うことでクライアント側で取得できることを意味することである。これらの基本点を留意して、図５は、ドメイン１００の登録ネーム・サーバで実行されるときの本発明の一実施例のフローチャートを示したものである。以下の説明において、外側ＮＳ１２０は図１に示すようにドメイン１００の登録ネーム・サーバである。

【００４２】実行は、外側ＮＳ１２０がドメイン１００に置かれているホスト（「登録ホスト」）のアドレスの照会を受信したときステップ３０５からスタートする。ステップ３１０で、外側ＮＳ１２０は要求されたホスト名に一致する所有者名をもつＳＸレコードがそのゾーン・データベースにあるかどうかをチェックする。そのようなレコードがデータベースになければ、実行はステップ３２０にジャンプする。データベースにレコードがあれば、ステップ３１５で、外側ＮＳ１２０は要求されたホストのセキュア・エクスチェンジャを示すＳＸレコードを応答に追加する。

【００４３】ステップ３２０で、外側ＮＳ１２０は要求されたホストのＡレコードがそのゾーン・データベースにあるかどうかを確かめるためにチェックする。要求されたホストのＡレコードがデータベースにあれば（つまり、要求されたホストのアドレスが公開され、見えるようになっている）、外側ＮＳ１２０はステップ３３５でホストのＡレコードを応答に追加し、ステップ３４０に進む。データベースにＡレコードがなければ（つまり、要求されたホストが保護ゾーン１８０に置かれている）、ステップ３２５で、外側ＮＳ１２０は照会すべき他のネーム・サーバがあれば、それを示しているＮＳレコード（または複数のレコード）を応答に追加する。外側ＮＳ１２０はステップ３３０で示すように、オプションとしてこれらのネーム・サーバのＡレコードを追加してから、ステップ３４０から続けることができる。

【００４４】ＳＸレコードがステップ３１５で応答に追加されたときは、ステップ３４０で外側ＮＳ１２０はオプションとしてＳＸレコードのデータ・フィールドに入っているセキュア・エクスチェンジャのＡレコードとＫＥＹレコードを応答に追加することも可能である。最後に、ステップ３４５で外側ＮＳ１２０は応答をリクエス

タに送付する。図１０は、要求されたホストのアドレスが公開され、見えるようになっている場合の応答の例を示す図である。図１１は、要求されたホストが保護ゾーンに置かれている場合の応答の例を示す図である。

【００４５】Ｊ　許可クライアントで実現される発明
図６、図７および図８は許可クライアント２１０で実行されるときの発明の種々実施例のフローチャートを示す図である。当業者ならば理解されるように、ここで説明している機能はハードウェアで実現することも、ソフトウェアで実現することもできる。前者の場合、このハードウェアには、汎用プロセッサ、マイクロプロセッサ、プログラム・ロジック・アレイ、アプリケーション専用集積回路、およびここで説明している機能を実行するのに十分な処理能力をもつ他のデバイスを含めることが可能である。後者の場合、このソフトウェアは任意の該当ハードウェア・プラットフォーム上で実行させることが可能であり、オブジェクト指向または手続き型プログラミング言語を含む、任意の該当プログラミング言語を使用して実現することが可能である。

【００４６】以下のセクションでは、本発明の２つの実施例を詳しく検討しているが、そこでは許可クライアント２１０上で実行されているアプリケーション２１５は内側ホスト１４０のアドレスの照会を行っている。最初の実施例では、ドメイン１００の１つのネーム・サーバを使用し、ネットワーク・トポロジは隠されていない（つまり、内側ホスト１４０のアドレスは１サーバ実施例では公開され、見えるようになっている）。言い換えれば、登録ネーム・サーバのデータベースは内側ホスト１４０のＡアドレスを含んでいる。第２の実施例では、ゾーンはネットワーク・トポロジを隠すように定義されており（つまり、内側ホスト１４０は保護ゾーン１８０に置かれている）、登録ネーム・サーバのデータベースは内側ホスト１４０のＡレコードをもっていない。その代わりに、このＡレコードは第２のサーバによって使用されるゾーン・データベースに置かれている。これらの実施例はフローチャートを通る異なった経路をたどっていくが、どちらもステップ４０５－４２５からスタートする。

【００４７】ステップ４０５で、リゾルバ２２５はアプリケーション２１５から照会を受信する。ステップ４１０で、リゾルバ２２５は内側ホスト１４０のドメインのネーム・サーバまでレフェラルチェーン(referral chain)をたどっていくことができるが、ローカル・サーバが再帰的サービスをサポートしていれば、照会をローカルＮＳ２５０に渡すことも可能である。いずれの場合も、リゾルバ２２５にはその後で、ステップ４１５で照会に対する応答が戻される。

【００４８】ステップ４２０で、リゾルバ２２５は応答にＳＸレコードがあるかどうかをチェックして確かめる。これらの実施例のどちらの場合も、要求されたホスト名に一致する所有者名をもつＳＸレコードが登録ネーム・サーバのデータベースに含まれていれば、リゾルバが受信する最初の応答（つまり、登録ネーム・サーバからの応答）にはＳＸレコードが入っている。これらの実施例の以下の説明では、このようなＳＸレコードが存在し、応答に含まれているものと想定している。当業者ならば理解されるように、セキュリティ上の目的から、ＳＸレコードは署名され、そのシグネーチャ（署名）は受信時に受信側で検証されるのが一般である。図１０は要求されたホストのアドレスが公開されて、見えるようになっている場合の応答例を示す図であり、図１１は要求されたホストが保護ゾーンに置かれている場合の応答例を示す図である。

【００４９】実行はステップ４２５から続けられ、そこでリゾルバ２２５は内側ホスト１４０のＡレコードが応答にあるかどうかをチェックして確かめる。２実施例が異なる経路をたどっていくのはこのステップからである。応答にＡレコードがなければ、実行はステップ４４０にジャンプするが、その詳細は「２サーバ実施例」のセクションで下述する。Ａレコードがあれば、実行はステップ４３０から続けられるが、その詳細は以下の「１サーバ実施例」のセクションで説明する。

【００５０】

【実施例】１．１サーバ実施例
要約して説明すると、この実施例では、１ネーム・サーバが使用され、ネットワーク・トポロジは隠されていない。図１を参照して説明すると、内側ＮＳ１３０は必要でなく、外側ＮＳ１２０のデータベースは内側ホスト１４０を含めて、ドメイン１００に置かれているマシンのレコードを含んでいる。従って、図６のステップ４１５では、アプリケーション２１５からのアドレス照会に対してリゾルバ２２５が受信する最初の応答には、内側ホスト１４０のＡレコードと、ファイアウォール１１０を対応するセキュア・エクスチェンジャとして示しているＳＸレコードが含まれている。図１０はこの応答の例を示す図である。

【００５１】「登録ネーム・サーバで実現される発明」のセクションで上述したように、応答はファイアウォール１１０のＡレコードとＫＥＹレコードを含んでいる場合もある。これらの追加レコードが応答になければ、リゾルバ２２５は必要に応じて追加の照会を行う（図６には図示せず）。また、上述したように、すべての該当ＳＩＧレコードが応答に含まれている（つまり、各レコード・タイプとレコード所有者名の組み合わせごとに１つのＳＩＧレコード）。リゾルバ２２５がこれらのレコードをすべて受信すると、実行がステップ４３０から続けれ、そこでリゾルバ２２５は図５に示すようなトンネル・マップ・エントリ５００を作成し、これは内側ホスト１４０へのメッセージを暗号化するために暗号プロセッサ２３０によって使用される。

【００５２】次に、図９の行２を参照して説明すると、トンネル・マップ・エントリ５００を作成するために、リゾルバ２２５は内側ホスト１４０のＡレコード内のデータをフィールド１　５１０内のデスティネーション・アドレスとして使用する。リゾルバ２２５は、それぞれＳＸレコードに示されているセキュア・エクスチェンジャ（つまり、ファイアウォール１１０）のＡレコードとＫＥＹレコード内のデータを使用してフィールド２　５２０とフィールド３　５３０を埋める。「リゾルバの機能」のセクションで説明したように、フィールド４　５４０はＳＸレコードに示されているセキュア・エクスチェンジャのカバレッジ有効範囲を示すために使用される。これは、ゾーン・データベースに置かれているときのＳＸレコードのオリジナル名を導き出し、それをフィールド４　５４０にストアすることによって行われる。従って、「オリジナル・データベース名」という用語はここでは、フィールド４　５４０の内容を意味するものとして用いられ、以下では、リゾルバ２２５がどのようにしてこの名前を導き出すかについて説明する。

【００５３】リゾルバ２２５はＳＸレコードのＳＩＧレコードのラベル・フィールドに入っているカウントを使用して、応答の中で送られたレコードの所有者名からラベルをいくつ残しておくべきかを判断する。例えば、ＳＸレコード（およびその関連ＳＩＧレコード）の所有者名がｅｎｇ．sun.com.であり、ラベル・フィールド・カウントが２であれば、オリジナル・データベース名は＊.sun.com. となる。カウントが３であれば、応答の中で送られるオリジナル・データベース名とレコードの所有者名はどちらもeng.sun.com.となる。ゾーン・データベースではワイルドカード名が使用されるのが代表的であるが、当業者ならば理解されるように、ワールドカード名は必須ではない。ゾーン・データベースにワイルドカードを使用していない本発明の実施例では、リゾルバ２２５はこれに代わる方法として、応答の中で送られたＳＸまたはＳＩＧレコードから名前を抜き出すといったように、他の方法でオリジナル・データベース名を導き出すこともできる。フィールド４　５４０にオリジナル・データベース名が満たされると、トンネル・マップ・エントリ５００は完成する。「リゾルバの機能」のセクションで説明したように、フィールド４　５４０はデータ構造の中の新規フィールドであり、そこにはアウトバウンド・セキュア・メッセージ情報が収められており、本発明の一実施例では、この情報を使用してＳＸレコードに示されたセキュア・エクスチェンジャのカバレッジ有効範囲を示している。

【００５４】次に、図６を参照して説明すると、トンネル・マップ・エントリ５００を作成した後、リゾルバ２２５はステップ４３５で内側ホスト１４０のアドレスをアプリケーション２１５に戻す。実行がここで終わると、トンネル・マップ・エントリ５００には、暗号プロセッサ２３０が内側ホスト１４０へのメッセージを暗号化するために必要な一切の情報が入っているので、アプリケーション２１５は内側ホスト１４０と機密に通信することが可能になる。１ネーム・サーバが使用され、ネットワーク・トポロジが隠されていない場合の実施例では、以上によって実行が完了する。

【００５５】２．２サーバ実施例

ネットワーク・トポロジが隠されている場合の実施例は、２ネーム・サーバを使用して実現することができる。図１を参照して説明すると、外側ＮＳ１２０はドメイン１００の登録ネーム・サーバとなり、ドメイン・データベースは内側ホスト１４０のＡレコードを含まないことになる。その代わりに、このレコードは保護ゾーン１８０の権限をもつネーム・サーバである、内側ＮＳ１３０によって使用されるゾーン・データベースに置かれることになる。従って、この実施例では、内側ホスト１４０のアドレスに関するアプリケーション２１５からの照会に対する最初の応答は外側ＮＳ１２０から送信される。図１１は、この応答の例を示す図である。外側ＮＳ１２０のデータベースは内側ホスト１４０のＡレコードを含んでいないので、リゾルバ２２５がステップ４１５で受信した最初の応答にはＡレコードが入っていない。しかし、この実施例では、応答にはファイアウォール１１０をセキュア・エクスチェンジャとして示すＳＸレコードと、内側ＮＳ１３０をゾーンの権限をもつネーム・サーバとして示す、少なくとも１つのＮＳレコードが入っている。従って、リゾルバ２２５がステップ４２５でＡレコードがあるかどうか応答をチェックしても、Ａレコードは見つからないので実行はステップ４４０にジャンプする。

【００５６】次に、図７を参照して説明すると、ステップ４４０でリゾルバ２２５はまだ照会されていないネーム・サーバ、つまり、外側ＮＳ１２０以外のネーム・サーバを収めているＮＳレコードがあるかどうか応答をチェックする。従って、この実施例では、実行がステップ４４０まで初めて到達すると、リゾルバ２２５は内側ＮＳ１３０を示すＮＳレコードとファイアウォール１１０を示すＳＸレコードを応答から探す。なお、この時点でＮＳレコードがなければ、エラーが発生しているので、実行は終了する。

【００５７】「登録ネーム・サーバで実現される発明」のセクションで上述したように、応答には内側ＮＳ１３０のＡレコードのほかに、ファイアウォール１１０のＡレコードとＫＥＹレコードも含まれている場合がある。これらの追加レコードが応答になければ、リゾルバ２２５は必要に応じて追加の照会（図８には示していない）を行う。また、上述したように、すべての該当ＳＩＧレコードはいずれかの応答に含まれている（つまり、各レコード・タイプとレコード所有者名の組み合わせごとに１つのＳＩＧレコード）。リゾルバ２２５がこれらのレ

コードすべてを受信すると、実行はステップ４４５から続行され、そこでリゾルバ２２５は図９に示すようにトンネル・マップ・エントリ５００を作成する。

【００５８】次に、図９の行３を参照して説明すると、トンネル・マップ・エントリ５００を作成するために、リゾルバ２２５は内側ＮＳ１３０のＡレコードに入っているデータをフィールド１　５１０内のデスティネーション・アドレスとして使用する。リゾルバ２２５は、それぞれＳＸレコードに示されたセキュア・エクスチェンジャ（つまり、ファイアウォール１１０）のＡレコードとＫＥＹレコードに入っているデータを使用してフィールド２　５２０とフィールド３　５３０を埋める。フィールド４　５４０を埋めるために、リゾルバ２２５はゾーン・データベースに置かれているときのＳＸレコードのオリジナル名を導き出す。リゾルバ２２５がどのようにしてこのオリジナル・データベース名を導き出すかの詳しい説明は「１サーバ実施例」のセクションに記載されている。

【００５９】次に、図７を参照して説明すると、トンネル・マップ・エントリ５００を作成した後、ステップ４５０でリゾルバ２２５は処理したばかりのＮＳレコードからのネーム・サーバ（つまり、内側ＮＳ１３０）を「最良の推量」としてＳＬＩＳＴ構造に挿入する。ＳＬＩＳＴの詳細は「リゾルバの機能」のセクションに説明されている。次に、図６を参照して説明すると、実行はステップ４１０にジャンプし、そこでネーム・サーバまでのレフェラルチェインは内側ＮＳ１３０（内側ホスト１４０のゾーンのネーム・サーバ）に通じることになる。そのあと、内側ホスト１４０のアドレスに関するアプリケーション２１５からの照会は最後のトンネル・マップ・エントリ５００のフィールド１　５１０、フィールド２　５２０、およびフィールド３　５３０を使用して暗号プロセッサ２３０によって暗号化される。照会が内側ＮＳ１３０に到達すると、サーバは標準応答（例えば、ＡレコードおよびＳ対応するＳＩＧレコード）をリクエスタに送信する。図１２はこの応答の例を示す図である。

【００６０】ステップ４１５で、リゾルバ２２５は応答を受信し、ステップ４２０で、リゾルバ２２５はＳＸレコードがあるかどうかをチェックする。ＳＸレコードがなければ、実行はステップ４５５にジャンプし（図８参照）、そこでリゾルバ２２５は内側ホスト１４０のＡレコードがあるかどうかをチェックする。そのようなＡレコードがなければ、実行は終了する。そうでなければ、ステップ４６０で、リゾルバ２２５はＳＸレコードによって作成され、そのオリジナル・データベース名が内側ホスト１４０の名前に一致しているエントリがトンネル・マップにあるかどうかをチェックする。そのようなエントリがなければ、ステップ４６５でリゾルバ２２５はホストのアドレスをアプリケーションに戻し、実行は終了する。一致するエントリがあれば、ステップ４７０でリゾルバ２２５は別のトンネル・マップ・エントリ５００を追加する。

【００６１】次に、図９の行４を参照して説明すると、リゾルバ２２５は内側ホスト１４０のＡレコード内のデータをフィールド１　５１０内のデスティネーション・アドレスとして使用する。他のフィールドを完成するために、リゾルバ２２５は、フィールド４　５４０内のオリジナル・データベース名が内側ホスト１４０の名前に最も多くの一致ラベルをもっている、既存のトンネル・マップ・エントリ５００を使用する。例えば、eng.sun.com が内側ホスト１４０の名前であれば、eng.sun.com は＊sun.com.よりも多くの一致ラベルをもつことになる。リゾルバ２２５は既存エントリからのフィールドを使用して、様々な方法で新規エントリを作成することができる。例えば、リゾルバ２２５はエントリを既存エントリから新規エントリにコピーすることも、あるいはリゾルバ２２５は単純にポインタを使用することもできる。

【００６２】トンネル・マップ・エントリ５００を作成した後、リゾルバ２２５はステップ４７５で内側ホスト１４０のアドレスをアプリケーション２１５に戻す。実行がここで終了していれば、アプリケーション２１５は、暗号プロセッサ２３０が内側ホスト１４０へのメッセージを暗号化するために必要とするすべての情報がトンネル・マップ・エントリに入っているので、内側ホスト１４０と機密に通信することが可能になる。２ネーム・サーバが使用され、ネットワーク・トポロジが隠されている場合の実施例では、以上により実行が完了する。

【００６３】Ｋ　その他の実施例

本発明は上述してきた２つの実施例に限定されるものではない。例えば、本発明は複数のゾーンを含むドメインで実現することが可能である。そのような実施例では、登録ネーム・サーバは照会を、権限をもつ複数のゾーン・ネーム・サーバに送ることができる。

【００６４】別の実施例では、本発明は私用ネットワーク内のセキュリティを保証するように実現することが可能である。当業者に公知であるように、ネーム・サーバ・ソフトウェアはスタンドアローン・ネットワークにインストールすることができる。そのような実施例では、該当のネーム・サーバは上述した登録ネーム・サーバと権限をもつネーム・サーバの機能を実行するように構成されることになる。

【００６５】さらに別の実施例では、リゾルバはホストのＡレコードを要求する前にＳＸレコードを要求することも可能である。そのような実施例では、ＳＸレコードは登録ネーム・サーバによって自動的に送信されないことになる。

【００６６】さらに別の実施例では、許可クライアントから保護ネーム・サーバへの照会はホストのアドレス以

外の情報に対するものにすることが可能である。この実施例では、登録ネーム・サーバからの応答は保護ネーム・サーバのゾーン・データベース内の情報に関するセキュア照会を送信するために使用できる。この実施例では、セキュア・エクスチェンジャのカバレッジ有効範囲を示すオリジナル・データベース名は、ネーム・サーバのトンネル・マップ・エントリだけが使用されるので必要でない。

【００６７】リゾルバ機能がアプリケーションに組み込まれているときは他の実施例も可能である。例えば、アプリケーションが作成するトンネル・マップはプログラムが実行中のときだけ存在させることができる。別の方法として、トンネル・マップを存続させるが、プログラムだけがアクセス可能にすることもできる（例えば、オペレーティング・システム２３５にはそのことを知らせないようにする）。

【００６８】さらに、開示した実施例の種々ステップは他の組み合わせで組み合わせることが可能である。登録ネーム・サーバからの応答が要求されたホストのアドレスを含み、トンネル・マップが既存エントリを含んでいて、オリジナル・データベース名が要求されたホストの名前と一致している場合には、そのような実施例は実現可能である。この実施例では、新規のトンネル・マップ・エントリは既存エントリを使用して、要求されたホストのために作成されることになる。

【００６９】当業者ならば理解されるように、これまでに説明してきた本発明の精神と範囲から逸脱しない限り、本発明はさらに別の実施例で実現することも可能である。なお、かかる実施例は請求の範囲に記載されている本発明の範囲内に属することはもちろんである。

【図面の簡単な説明】

【図１】本発明の実施例を実行させることができる代表的なインターネット構成を示す図である。

【図２】本発明が実現されているクライアントの構成例を示す図である。

【図３】本発明が実現されているクライアントの構成例を示す図である。

【図４】本発明が実現されているクライアントの構成例を示す図である。

【図５】ドメインの登録ネーム・サーバで実行されるときの本発明の一実施例のフローチャートである。

【図６】クライアントで実行されるときの本発明の一実施例のフローチャートである。

【図７】クライアントで実行されるときの本発明の一実施例のフローチャートである。

【図８】クライアントで実行されるときの本発明の一実施例のフローチャートである。

【図９】本発明の一実施例によって使用されるトンネル・マップの例を示す図である。

【図１０】クライアントからのアドレス照会に対する応答の例を示す図である。

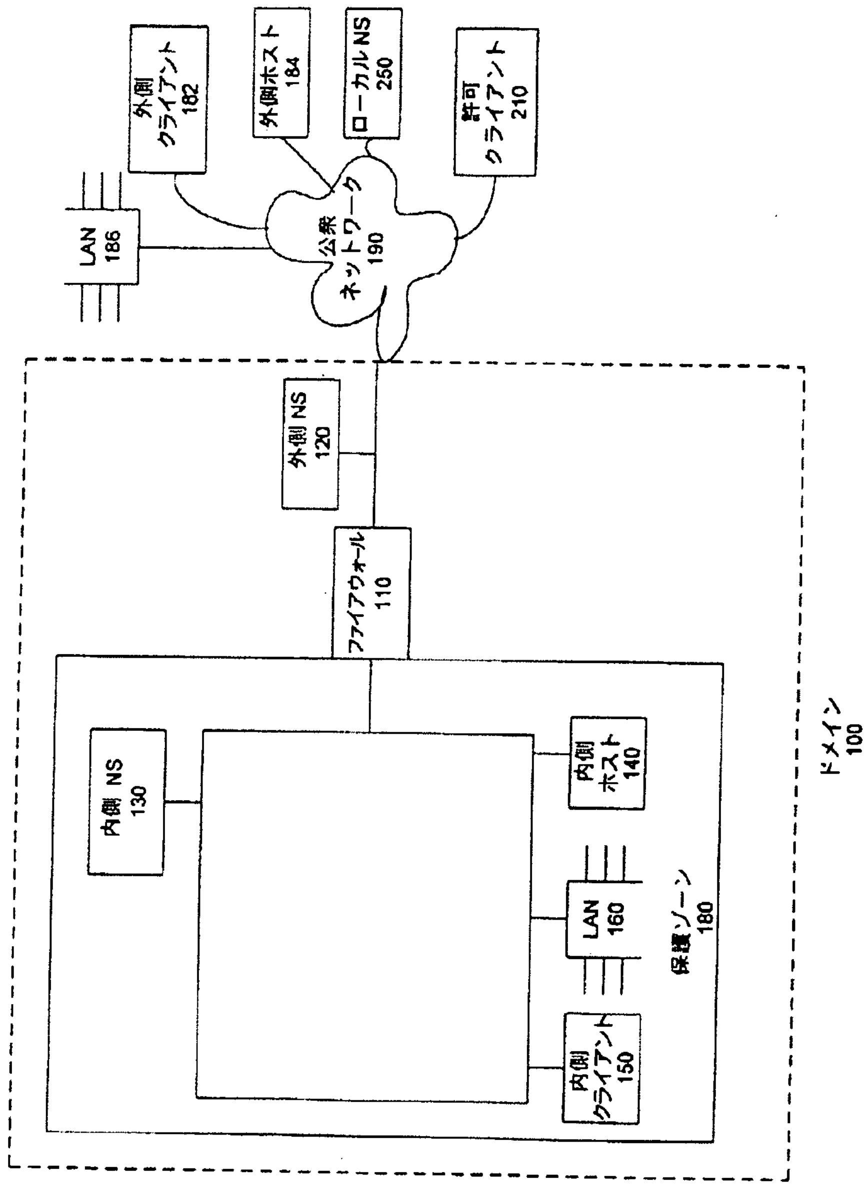
【図１１】クライアントからのアドレス照会に対する応答の例を示す図である。

【図１２】クライアントからのアドレス照会に対する応答の例を示す図である。

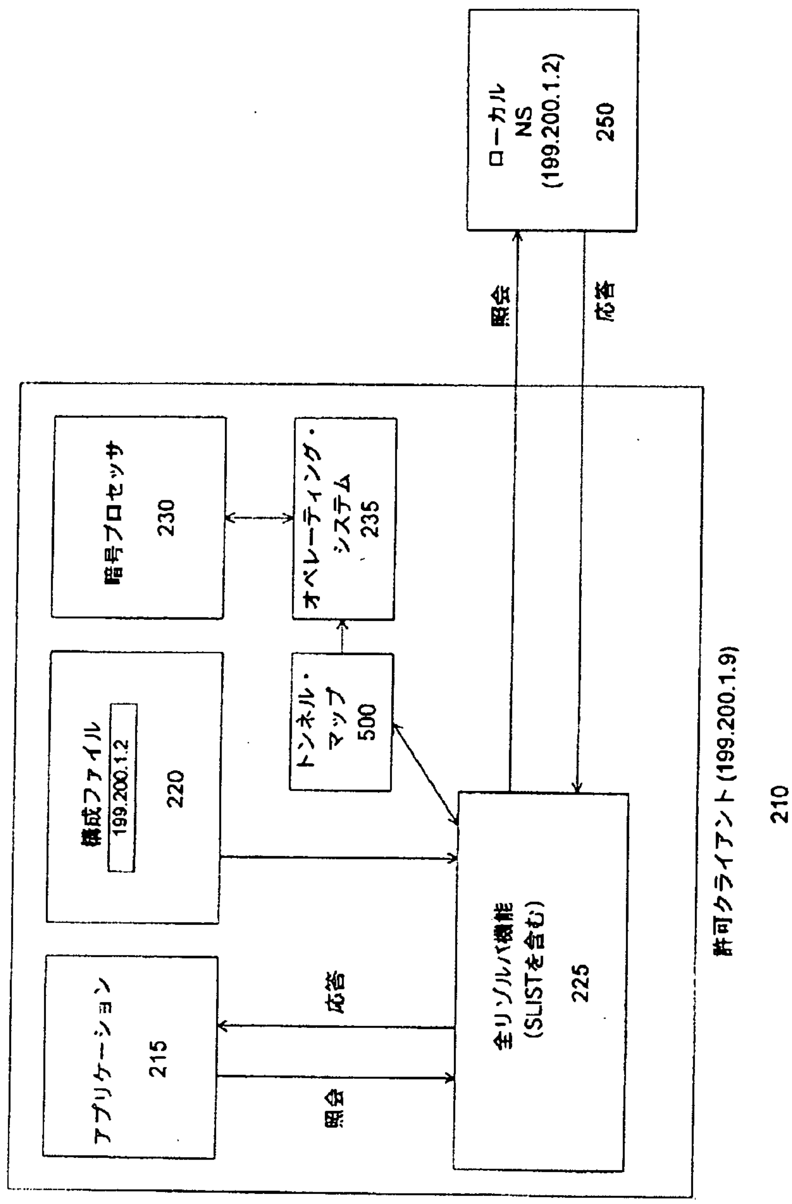
【符号の説明】

１００　ドメイン
１１０　ファイアウォール
１２０　外側ＮＳ
１３０　内側ＮＳ
１４０　保護ホスト
１５０　内側クライアント
１６０　ＬＡＮ
１８０　保護ゾーン
１８２　外側クライアント
１８４　外側ホスト
１８６　ＬＡＮ
１９０　公衆ネットワーク
２１０　許可クライアント
２１５　アプリケーション
２２０　構成ファイル
２２５　リゾルバ
２３０　暗号プロセッサ
２５０　ローカルＮＳ
５００　トンネル・マップ・エントリ

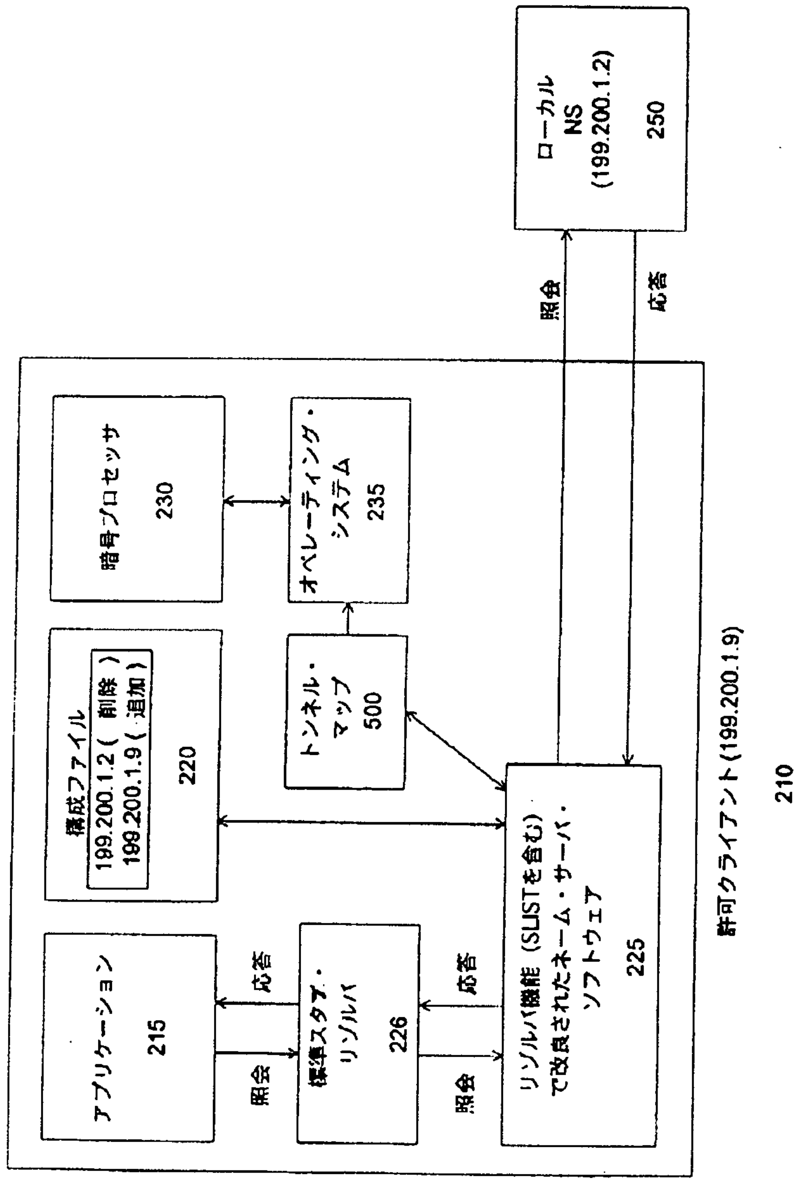
【図1】


外側クライアント 182
外側ホスト 184
ローカルNS 250
許可クライアント 210
LAN 186
公衆ネットワーク 190
外側NS 120
ファイアウォール 110
内側NS 130
内側ホスト 140
LAN 160
内側クライアント 150
保護ゾーン 180
ドメイン 100

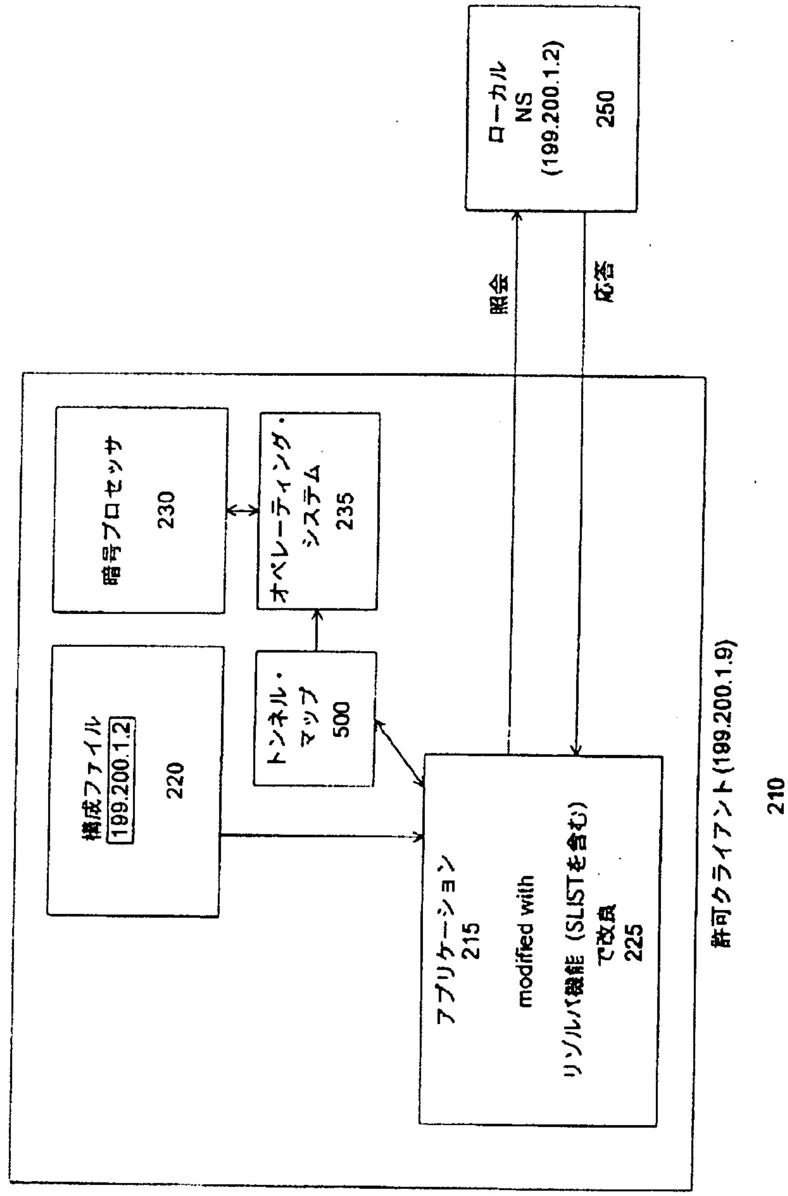
【図2】


ローカル
NS
(199.200.1.2)
250
照会
応答
暗号プロセッサ
230
オペレーティング・
システム
235
構成ファイル
199.200.1.2
220
トンネル・
マップ
500
アプリケーション
215
応答
照会
全リゾルバ機能
(SLISTを含む)
225
許可クライアント(199.200.1.9)
210

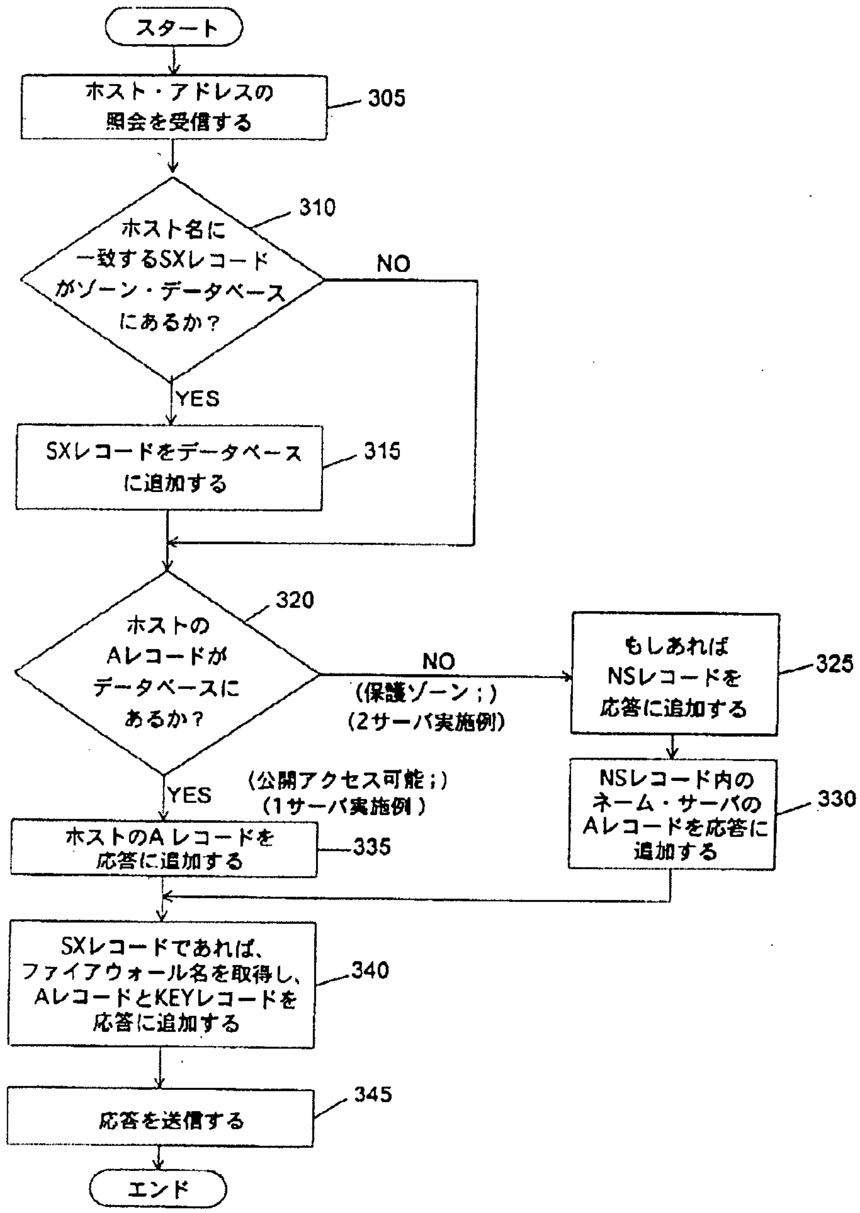
【図3】


ローカル
NS
(199.200.1.2)
250
照会
応答
暗号プロセッサ
230
オペレーティング・
システム
235
構成ファイル
199.200.1.2（削除）
199.200.1.9（追加）
220
トンネル・
マップ
500
アプリケーション
215
照会
応答
標準スタブ・
リゾルバ
226
照会
応答
リゾルバ機能（SLISTを含む）
で改良されたネーム・サーバ・
ソフトウェア
225
許可クライアント(199.200.1.9)
210

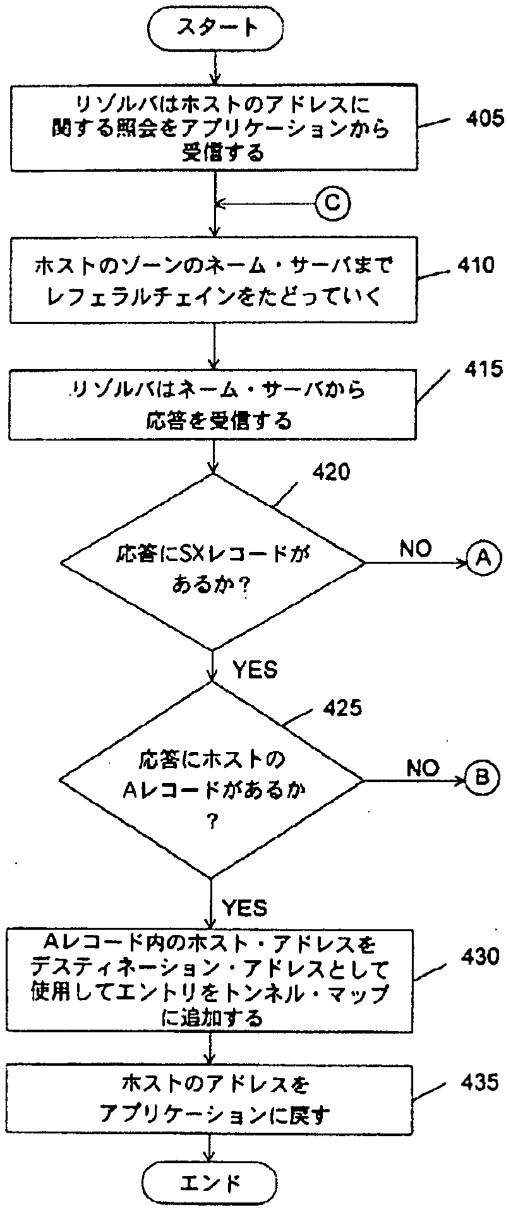
【図4】


ローカル
NS
(199.200.1.2)
250
照会
応答
暗号プロセッサ
230
オペレーティング・
システム
235
構成ファイル
199.200.1.2
220
トンネル・
マップ
500
アプリケーション
215
modified with
リゾルバ機能（SLISTを含む）
で改良
225
許可クライアント(199.200.1.9)
210

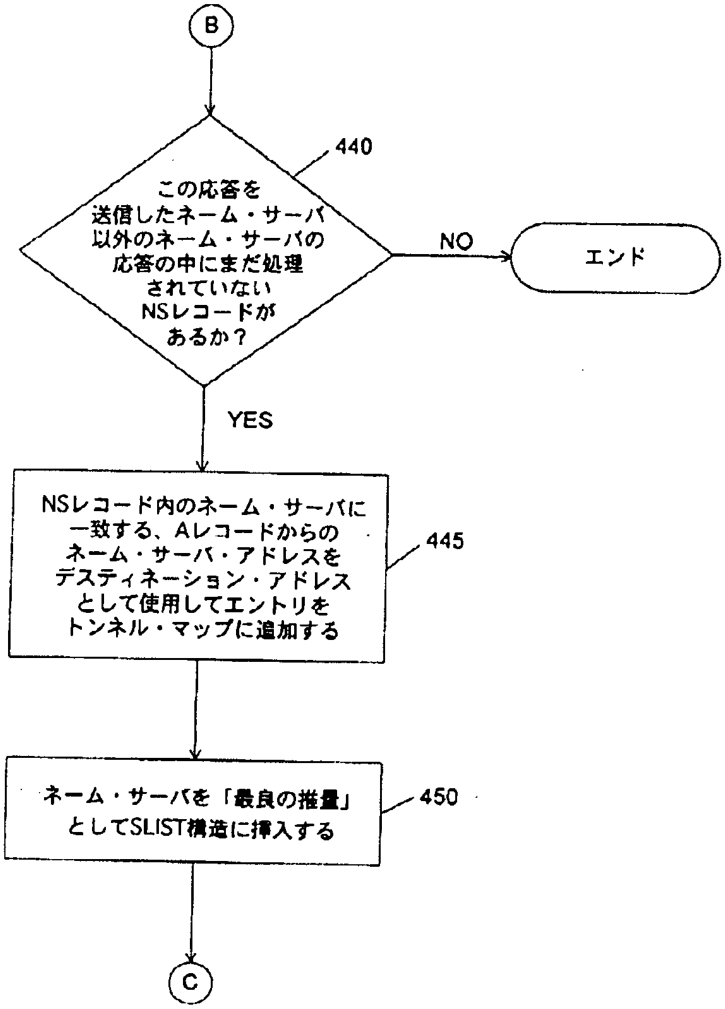
【図5】


スタート
ホスト・アドレスの照会を受信する
305
310
ホスト名に一致するSXレコードがゾーン・データベースにあるか？
NO
YES
SXレコードをデータベースに追加する
315
320
ホストのAレコードがデータベースにあるか？
NO
(保護ゾーン；)
(2サーバ実施例)
もしあればNSレコードを応答に追加する
325
YES
(公開アクセス可能；)
(1サーバ実施例)
ホストのAレコードを応答に追加する
335
NSレコード内のネーム・サーバのAレコードを応答に追加する
330
SXレコードであれば、ファイアウォール名を取得し、AレコードとKEYレコードを応答に追加する
340
応答を送信する
345
エンド

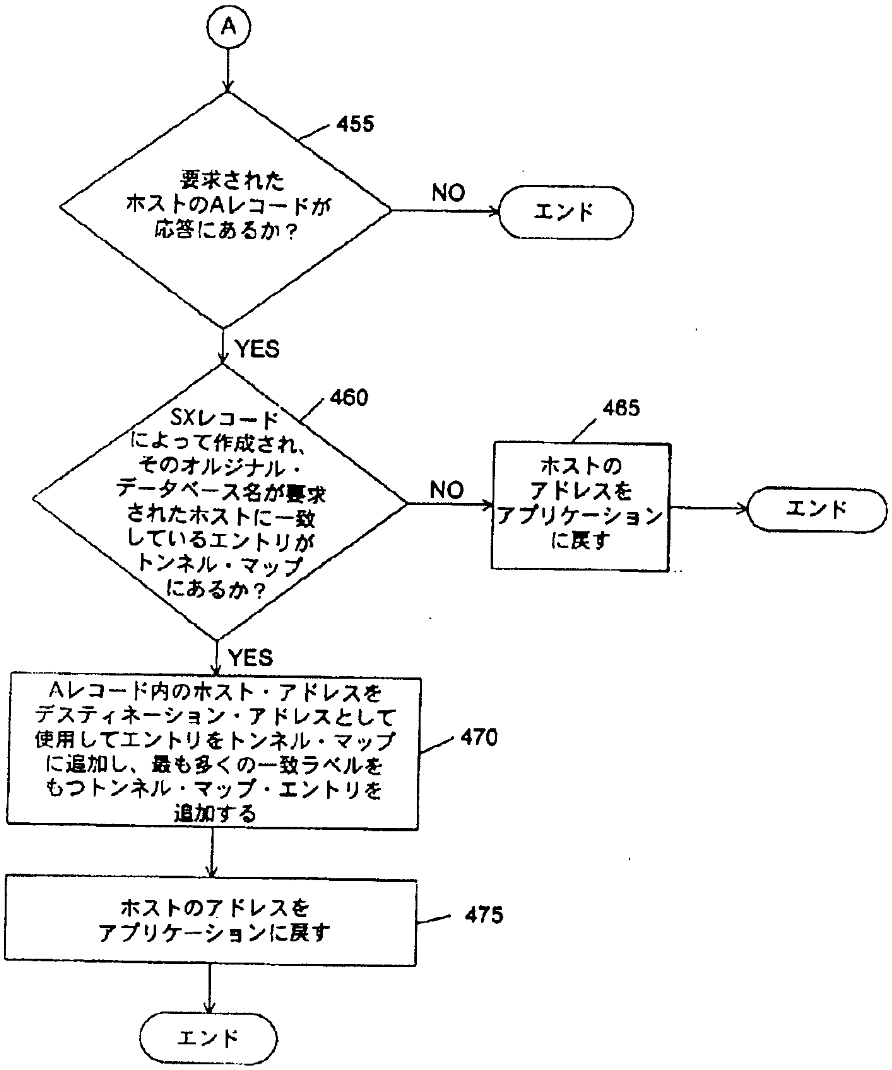
【図6】


スタート
リゾルバはホストのアドレスに関する照会をアプリケーションから受信する
405
C
ホストのゾーンのネーム・サーバまでレフェラルチェインをたどっていく
410
リゾルバはネーム・サーバから応答を受信する
415
420
応答にSXレコードがあるか？
NO
A
YES
425
応答にホストのAレコードがあるか？
NO
B
YES
Aレコード内のホスト・アドレスをデスティネーション・アドレスとして使用してエントリをトンネル・マップに追加する
430
ホストのアドレスをアプリケーションに戻す
435
エンド

【図7】


B
440
この応答を
送信したネーム・サーバ
以外のネーム・サーバの
応答の中にまだ処理
されていない
NSレコードが
あるか？
NO
エンド
YES
NSレコード内のネーム・サーバに
一致する、Aレコードからの
ネーム・サーバ・アドレスを
デスティネーション・アドレス
として使用してエントリを
トンネル・マップに追加する
445
ネーム・サーバを「最良の推量」
としてSLIST構造に挿入する
450
C

【図8】


A
455
要求された
ホストのAレコードが
応答にあるか？
NO
エンド
YES
460
SXレコード
によって作成され、
そのオルジナル・
データベース名が要求
されたホストに一致
しているエントリが
トンネル・マップ
にあるか？
NO
465
ホストの
アドレスを
アプリケーション
に戻す
エンド
YES
Aレコード内のホスト・アドレスを
デスティネーション・アドレスとして
使用してエントリをトンネル・マップ
に追加し、最も多くの一致ラベルを
もつトンネル・マップ・エントリを
追加する
470
ホストのアドレスを
アプリケーションに戻す
475
エンド

【図９】

	フィールド1 510	フィールド2 520	フィールド3 530	フィールド4 540
行1 （内容の記述）	デスティネーション・アドレス	ファイアウォールのアドレス	公開キー または 公開キー名	このエントリを作成したSXレコードの導き出されたオリジナル・データベース名
行2 （1サーバ実施例）	Aレコード内にあって要求されたホストのホスト・アドレスを使用する	SXレコード内のファイアウォールのAレコードを使用する	SXレコード内のファイアウォールのKEYレコードを使用する	SX レコードのSIGレコード内のラベル・カウントを使用してワイルドカード名を生成する
行3 （2サーバ実施例の第1エントリ）	Aレコード内にあってNSレコード内のネーム・サーバに一致するネーム・サーバ・アドレスを使用する	SXレコード内のファイアウォールのAレコードを使用する	フィールド4内の最も多くの一致ラベルをもつ既存エントリを使用し、それをコピーし、それを指し示す、など	SXレコードのSIGレコード内のラベル・カウントを使用してワイルドカード名を生成する
行4 （2サーバ実施例の第2エントリ）	Aレコード内にあって要求されたホストのホスト・アドレス	フィールド4内の最も多くの一致ラベルをもつ既存エントリを使用し、それをコピーし、それを指し示す、など	フィールド4内の最も多くの一致ラベルをもつ既存エントリを使用し、それをコピーし、それを指し示す、など	フィールド4内の最も多くの一致ラベルをもつ既存エントリを使用し、それをコピーし、それを指し示す、など

エントリ・マップ・エントリ

500

【図10】

セクション	所有者名	レコード・タイプ	データ
ヘツダ	＜ヘッダ＞		
照会	＜照会＞		
返答	＜内側ホス140＞	A	＜内側ホスト140のアドレス＞
	＜内側ホス140＞	SIG	＜SIGデータ＞
権限	＜内側ホス140＞	SX	＜ファイアウォール110のID＞
	＜内側ホス140＞	SIG	＜SIGデータ；ラベル・カウント=2＞
追加	＜ファイアウォール110＞	A	＜ファイアウォール110のアドレス＞
	＜ファイアウォール110＞	SIG	＜SIGデータ＞
	＜ファイアウォール110＞	KEY	＜ファイアウォール110のキー・データ＞
	＜ファイアウォール110＞	SIG	＜SIGデータ＞

【図11】

セクション	所有者名	レコード・タイプ	データ
ヘツダ	＜ヘッダ＞		
照会	＜照会＞		
返答	＜ブランク＞		
権限	＜ドメイン100＞	NS	＜内側NS 130の名前＞
	＜ドメイン100＞	SIG	＜SIGデータ＞
	＜内側ホスト140＞	SX	＜ファイアウォール110のID＞
	＜内側ホスト140＞	SIG	＜SIGデータ；ラベル・カウント=2＞
追加	＜内側NS 130＞	A	＜内側NS 130のアドレス＞
	＜内側NS 130＞	SIG	＜SIGデータ＞
	＜ファイアウォール110＞	A	＜ファイアウォール110のアドレス＞
	＜ファイアウォール110＞	SIG	＜SIGデータ＞
	＜ファイアウォール110＞	KEY	＜ファイアウォール110のキー・データ＞
	＜ファイアウォール110＞	SIG	＜SIGデータ＞

【図12】

セクション	所有者名	レコード・タイプ	データ
ヘツダ	<ヘッダ>		
照会	<照会>		
返答	<内側ホスト140> <内側ホスト140>	A SIG	<内側ホスト140のアドレス> <SIGデータ>
権限	<ブランク>		
追加	<ブランク>		

フロントページの続き

(51)Int.Cl.[6]　　　識別記号　　　FI
H04L 12/56

(71)出願人 591064003
901 SAN ANTONIO ROAD
PALO ALTO, CA 94303, U.S.A.

(72)発明者 トーマス マークソン
アメリカ合衆国 94402 カリフォルニア州 サン マテオ マウンツ ロード 30 アパートメント 206

05-28-14

IFW

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.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	13/615,557
Filing Date	09-13-2012
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Attorney Docket Number	77580-177
Total Number of Pages in This Submission	

ENCLOSURES (*Check all that apply*)

- [ ] Fee Transmittal Form
  - [ ] 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

12 Boxes of Non Patent Literature; 11 Foreign Publication References. The Request for Continued Examination is being electronically filed on May 27, 2014 and all fees due will be paid at the time of the RCE filing.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	McDermott, Will @ Emery		
Signature	/Toby H. Kusmer/		
Printed name	Toby H. Kusmer		
Date	May 27, 2014	Reg. No.	26,418

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	

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.

Application Number	Application/Control No.	Applicant(s)/Patent under Reexamination
	13/615,557	LARSON ET AL.

Document Code - DISQ	**Internal Document – DO NOT MAIL**

TERMINAL DISCLAIMER	☒ APPROVED	☐ DISAPPROVED
Date Filed : 05-27-2014	**This patent is subject to a Terminal Disclaimer**	

Approved/Disapproved by:

Dorethea Lawrence --3-- approved

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

23630 7590 06/10/2014
McDermott Will & Emery
The McDermott Building
500 North Capitol Street, N.W.
Washington, DC 20001

EXAMINER	
LIM, KRISNA	
ART UNIT	PAPER NUMBER
2453	

DATE MAILED: 06/10/2014

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/615,557	09/13/2012	Victor Larson	077580-0177	1089

TITLE OF INVENTION: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	09/10/2014

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

23630 7590 06/10/2014

McDermott Will & Emery
The McDermott Building
500 North Capitol Street, N.W.
Washington, DC 20001

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/615,557	09/13/2012	Victor Larson	077580-0177	1089

TITLE OF INVENTION: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	09/10/2014

EXAMINER	ART UNIT	CLASS-SUBCLASS
LIM, KRISNA	2453	713-162000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
   - ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
   - ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
   (1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
   (2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
   1 ______________________
   2 ______________________
   3 ______________________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies ______________

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number ___________ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ Applicant certifying micro entity status. See 37 CFR 1.29
  NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ❑ Applicant asserting small entity status. See 37 CFR 1.27
  NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ❑ Applicant changing to regular undiscounted fee status.
  NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature ______________________ Date ______________________

Typed or printed name ______________________ Registration No. ______________________

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.
13/615,557	09/13/2012	Victor Larson	077580-0177	1089

23630 7590 06/10/2014

McDermott Will & Emery
The McDermott Building
500 North Capitol Street, N.W.
Washington, DC 20001

EXAMINER	
LIM, KRISNA	
ART UNIT	**PAPER NUMBER**
2453	

DATE MAILED: 06/10/2014

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. 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, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. 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.

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.

Notice of Allowability	Application No. 13/615,557	Applicant(s) LARSON ET AL.	
	Examiner KRISNA LIM	Art Unit 2453	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the RCE filed 05/27/2014*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on______.
2. ☐ 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.
3. ☒ The allowed claim(s) is/are *1,2,4-10,12 and 14-37*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   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)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☐ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/KRISNA LIM/
Primary Examiner, Art Unit 2453

1. The present application is being examined under the pre-AIA first to invent provisions.

2. Pursuant to 37 C.F.R 1.109 and M.P.E.P 1302.14, the following is an Examiner's Statement of Reasons for Allowance:

Kiuchi discloses that the C-HTTP name server stores the IP address and public key of a particular computer in a data structure that maps the name of the particular computer to the corresponding IP address and public key. Kiuchi discloses that the client-side proxy sends a request to the C-HTTP, where the request is asking the C-HTTP server for permission to establish a connection with a server-side proxy.

Wesinger describes a system in which a configuration file is stored on a series of firewalls. The configuration files store security information by domain name and use the domain name to determine if a particular request is to be allowed.
Moreover, Wesinger discloses the following sequence: (i) a request is received by the firewall/DNS server, (ii) the domain name in the request is looked up in the configuration file, (iii) if the connection is allowed, then the firewall/DNS server may invoke code that performs channel processing, which includes encryption.

Wesinger discloses that DNS propagation happens in a normal manner, but also teaches that the DNS propagation happens through the firewall servers, and the DNS propagation is subject to the allowance or denies connection rules.

In Examiner's opinion, both Kiuchi and Wesinger may not clearly disclose the feature of " (1) intercepting from the client device a request to look up an IP address corresponding to a domain name associated; (2) determining whether the request to look up the IP address transmitted in step (1) corresponds to a device that accepts an encrypted channel connection with the client device; and in response to determining, in step (2), that the request to look up the IP address in step (2) corresponds to a device that accepts an encrypted communications channel connection with the client device, providing provisioning information required to initiate the creation of the encrypted communications channel between the client device and the target device such that the encrypted communications channel supports secure data communications transmitted between the two devices, the client device being a device at which a user accesses the encrypted communications channel."

Examiner considers the applicants' claims 1-2, 4-10, 12, 14-37 to be allowable based on Examiner's understanding and Examiner's opinion should not be imputed to the concession of the prior arts and the exhaustion of the prior arts for determining the patentability of any or all claims.

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

May 29, 2014

/Krisna Lim/

Primary Examiner Art Unit 2453

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13615557	LARSON ET AL.
	Examiner	**Art Unit**
	KRISNA LIM	2453

CPC- SEARCHED

Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED

Symbol	Date	Examiner

US CLASSIFICATION SEARCHED

Class	Subclass	Date	Examiner
709	222-227	07/25/2013	kl
709	222-227	05/29/2013	kl

SEARCH NOTES

Search Notes	Date	Examiner
Inventors	07/25/2013	kl
Inventors	05/29/2014	kl

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
709	222-227	05/29/2014	kl

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13615557	LARSON ET AL.
	Examiner	**Art Unit**
	KRISNA LIM	2453

CPC						
Symbol					**Type**	**Version**
H04L		61	/	1511	I	2013-01-01
H04L		29	/	12216	I	2013-01-01
H04L		61	/	303	I	2013-01-01
H04L		63	/	0272	I	2013-01-01
H04L		29	/	12066	I	2013-01-01
H04L		29	/	12594	I	2013-01-01
H04L		63	/	04	I	2013-01-01
H04L		45	/	24	I	2013-01-01
H04L		29	/	12783	I	2013-01-01
H04L		63	/	1408	I	2013-01-01
H04L		63	/	1458	I	2013-01-01
H04L		29	/	1232	I	2013-01-01
H04L		63	/	164	A	2013-01-01
H04L		41	/	00	I	2013-01-01
H04L		45	/	00	I	2013-01-01
H04L		61	/	2092	I	2013-01-01
H04L		61	/	35	I	2013-01-01
H04L		61	/	2007	I	2013-01-01
H04L		63	/	08	I	2013-01-01
H04L		63	/	0428	I	2013-01-01
H04L		61	/	2076	I	2013-01-01
H04L		67	/	14	F	2013-01-01
H04L		45	/	28	I	2013-01-01
H04L		63	/	0407	I	2013-01-01
G06F		21	/	606	I	2013-01-01
H04L		63	/	0227	I	2013-01-01
H04L		29	/	12301	I	2013-01-01
H04L		63	/	1416	I	2013-01-01
H04L		63	/	1466	I	2013-01-01
H04L		29	/	12801	I	2013-01-01
H04L		63	/	105	A	2013-01-01

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 34	
/KRISNA LIM/ Primary Examiner.Art Unit 2453 (Primary Examiner)	05/29/2014 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 26, 27

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13615557	LARSON ET AL.
	Examiner	**Art Unit**
	KRISNA LIM	2453

H04L	61	/	6004	I	2013-01-01

CPC Combination Sets				
Symbol	**Type**	**Set**	**Ranking**	**Version**
/				
/				

NONE (Assistant Examiner) (Date)	**Total Claims Allowed:** 34	
/KRISNA LIM/ Primary Examiner.Art Unit 2453 05/29/2014 (Primary Examiner) (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 26, 27

Issue Classification

Application/Control No.	Applicant(s)/Patent Under Reexamination
13615557	LARSON ET AL.
Examiner	**Art Unit**
KRISNA LIM	2453

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**
709	222

INTERNATIONAL CLASSIFICATION					
CLAIMED					**NON-CLAIMED**
G	0	6	F	15 / 173 (2006.01.01)	

CROSS REFERENCE(S)

CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
709	223	223	224	225	226
709	227				

NONE (Assistant Examiner) (Date)	**Total Claims Allowed:** 34	
/KRISNA LIM/ Primary Examiner.Art Unit 2453 05/29/2014 (Primary Examiner) (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 26, 27

Issue Classification	**Application/Control No.**	**Applicant(s)/Patent Under Reexamination**
	13615557	LARSON ET AL.
	Examiner	**Art Unit**
	KRISNA LIM	2453

☐ **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
1	1	14	17	16	33										
2	2	15	18	17	34										
	3	21	19	18	35										
3	4	22	20	19	36										
4	5	23	21	20	37										
5	6	24	22												
6	7	25	23												
7	8	26	24												
8	9	27	25												
9	10	28	26												
	11	29	27												
10	12	30	28												
	13	31	29												
11	14	32	30												
12	15	33	31												
13	16	34	32												

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 34	
/KRISNA LIM/ Primary Examiner.Art Unit 2453 (Primary Examiner)	05/29/2014 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 26, 27

Index of Claims	**Application/Control No.** 13615557	**Applicant(s)/Patent Under Reexamination** LARSON ET AL.
	Examiner KRISNA LIM	**Art Unit** 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	07/25/2013	11/06/2013	02/19/2014	05/29/2014					
1	1	✓	✓	✓	=					
2	2	✓	✓	✓	=					
	3	✓	-		-					
3	4	✓	✓	✓	=					
4	5	✓	✓	✓	=					
5	6	✓	✓	✓	=					
6	7	✓	✓	✓	=					
7	8	✓	✓	✓	=					
8	9	✓	✓	✓	=					
9	10	✓	✓	✓	=					
	11	✓	-	-	-					
10	12	✓	✓	✓	=					
	13	✓	-	-	-					
11	14	✓	✓	✓	=					
12	15	✓	✓	✓	=					
13	16	✓	✓	✓	=					
14	17	✓	✓	✓	=					
15	18	✓	✓	✓	=					
21	19	✓	✓	✓	=					
22	20	✓	✓	✓	=					
23	21		✓	✓	=					
24	22		✓	✓	=					
25	23		✓	✓	=					
26	24		✓	✓	=					
27	25		✓	✓	=					
28	26		✓	✓	=					
29	27		✓	✓	=					
30	28		✓	✓	=					
31	29		✓	✓	=					
32	30		✓	✓	=					
33	31		✓	✓	=					
34	32		✓	✓	=					
16	33		✓	✓	=					
17	34		✓	✓	=					
18	35		✓	✓	=					
19	36		✓	✓	=					

Index of Claims	Application/Control No. 13615557	Applicant(s)/Patent Under Reexamination LARSON ET AL.
	Examiner KRISNA LIM	Art Unit 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	07/25/2013	11/06/2013	02/19/2014	05/29/2014					
20	37		✓	✓	=					

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.
13/615,557	09/13/2012	Victor Larson	077580-0177	1089

23630 7590 07/09/2014
McDermott Will & Emery
The McDermott Building
500 North Capitol Street, N.W.
Washington, DC 20001

EXAMINER	
LIM, KRISNA	
ART UNIT	**PAPER NUMBER**
2453	
NOTIFICATION DATE	**DELIVERY MODE**
07/09/2014	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

Supplemental Notice of Allowability	**Application No.** 13/615,557	**Applicant(s)** LARSON ET AL.	
	Examiner KRISNA LIM	**Art Unit** 2453	**AIA (First Inventor to File) Status** No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the RCE filed 05/27/2014*.

   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on______.

2. ☐ 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.

3. ☒ The allowed claim(s) is/are *1,2,4-10,12 and 14-37*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:

   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)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☐ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/KRISNA LIM/
Primary Examiner, Art Unit 2453

1. The present application is being examined under the pre-AIA first to invent provisions.

2 Pursuant to 37 C.F.R 1.109 and M.P.E.P 1302.14, the following is an Examiner's Statement of Reasons for Allowance:

Kiuchi discloses that the C-HTTP name server stores the IP address and public key of a particular computer in a data structure that maps the name of the particular computer to the corresponding IP address and public key. Kiuchi discloses that the client-side proxy sends a request to the C-HTTP, where the request is asking the C-HTTP server for permission to establish a connection with a server-side proxy.

Wesinger describes a system in which a configuration file is stored on a series of firewalls. The configuration files store security information by domain name and use the domain name to determine if a particular request is to be allowed.

Moreover, Wesinger discloses the following sequence: (i) a request is received by the firewall/DNS server, (ii) the domain name in the request is looked up in the configuration file, (iii) if the connection is allowed, then the firewall/DNS server may invoke code that performs channel processing, which includes encryption.

Wesinger discloses that DNS propagation happens in a normal manner, but also teaches that the DNS propagation happens through the firewall servers, and the DNS propagation is subject to the allowance or denies connection rules.

In Examiner's opinion, both Kiuchi and Wesinger may not clearly disclose the feature of"

(1) intercepting from the client device a request to look up an IP address corresponding to a domain name associated; (2) determining whether the request to look up the IP address transmitted in step (1) corresponds to a device that accepts an encrypted channel connection with the client device; and in response to determining, in step (2), that the request to look up the IP address in step (2) corresponds to a device that accepts an encrypted communications channel connection with the client device, providing provisioning information required to initiate the creation of the encrypted communications channel between the client device and the target device such that the encrypted communications channel supports secure data communications transmitted between the two devices, the client device being a device at which a user accesses the encrypted communications channel."

Examiner considers the applicants' claims 1-2, 4-10, 12, 14-37 to be allowable based on Examiner's understanding and Examiner's opinion should not be imputed to the concession of the prior arts and the exhaustion of the prior arts for determining the patentability of any or all claims.

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.

Kl
July 01, 2014

/Krisna Lim/
Primary Examiner Art Unit 2453

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

OIPE MAY 27 2014 PATENT & TRADEMARK OFFICE

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; 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.

[ ] The Commissioner is authorized to charge any required fees to Deposit Account 50-1133.

[X] Information Disclosure Statement is being filed with the Request for Continued Examination, which was electronically filed on May 27, 2014 and at that time, all fees due, were paid. However, the Commissioner is hereby authorized to charge any 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/

Date: May 27, 2014

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 52498342-1.077580.0177

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT VS. APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	**13/615,557**
Filing Date	**09-13-2012**
First Named Inventor	**Victor Larson**
Art Unit	**2453**
Examiner Name	**Krisna Lim**
Docket Number	**77580-177 (VRNK-0001CP3CON8)**

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
	A179	RE39,360	10/17/2006	Aziz et al.	
	A180	5,416,842	05/16/1995	Aziz	
	A181	5,420,926	05/30/1995	Low et al.	
	A182	5,444,782	08/22/1995	Adams, Jr. et al.	
	A183	5,455,861	10/03/1995	Faucher et al.	
	A184	5,530,758	06/25/1996	Marino, Jr. et al.	
	A185	5,623,601	04/22/1997	Vu	
	A186	5,636,139	06/03/1997	McLaughlin et al.	
	A187	5,689,566	11/18/1997	Nguyen	
	A188	5,781,550	07/14/1998	Templin et al.	
	A189	5,805,820	09/08/1998	Bellovin et al.	
	A190	5,812,670	09/22/1998	Micali	
	A191	5,884,270	03/16/1999	Walker et al.	
	A192	5,889,863	03/30/1999	Weber	
	A193	5,915,087	06/22/1999	Hammond et al.	
	A194	5,940,393	08/17/1999	Duree et al.	
	A195	5,961,593	10/05/1999	Gabber et al.	
	A196	5,974,454	10/26/1999	Apfel et al.	
	A197	6,003,084	12/14/1999	Green et al.	
	A198	6,012,088	06/04/2000	Li et al.	
	A199	6,016,504	01/18/2000	Arnold et al.	
	A200	6,023,510	02/08/2000	Epstein	
	A201	6,032,118	02/29/2000	Tello et al.	
	A202	6,055,236	04/25/200	Nessett et al.	
	A203	6,055,518	04/25/2000	Franklin et al.	
	A204	6,055,575	04/25/2000	Paulsen et al.	
	A205	6,073,175	06/06/2000	Tavs et al.	
	A206	6,111,883	08/29/2000	Terada et al.	
	A207	6,148,342	11/14/2000	Ho	
	A208	6,151,628	11/21/2000	Xu et al.	
	A209	6,154,839	11/28/2000	Arrow et al.	
	A210	6,182,072	01/30/2001	Leak et al.	
	A211	6,182,141	01/30/2001	Blum et al.	
	A212	6,199,122	03/06/2001	Wilson	
	A213	6,225,993	05/01/2001	Lindblad et al.	
	A214	6,298,383	10/02/2001	Gutman et al.	
	A215	6,345,361	02/05/2002	Jerger et al.	

/Krisna Lim/ 07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	A216	6,366,912	04/02/2002	Wallent et al.	
	A217	6,421,732	07/16/2002	Alkhatib et al.	
	A218	6,426,955	07/30/2002	Gossett et al.	
	A219	6,438,127	08/20/2002	Le Goff et al.	
	A220	6,449,272	09/10/2002	Chuah et al.	
	A221	6,453,034	09/17/2002	Donovan et al.	
	A222	6,490,290	12/03/2002	Zhang et al.	
	A223	6,496,491	12/17/2002	Chuah et al.	
	A224	6,564,261	05/13/2003	Gudjonsson et al.	
	A225	6,590,588	07/08/2003	Lincke et al.	
	A226	6,591,306	07/08/2003	Redlich	
	A227	6,606,660	08/12/2003	Bowman-Amuah	
	A228	6,609,196	08/19/2003	Dickinson III et al.	
	A229	6,636,505	10/21/2003	Wang et al.	
	A230	6,640,302	10/28/2003	Subramaniam et al.	
	A231	6,643,701	11/04/2003	Aziz et al.	
	A232	6,687,823	02/03/2004	Al-Salqan et al.	
	A233	6,693,878	02/17/2004	Daruwalla et al.	
	A234	6,751,729	06/15/2004	Giniger et al.	
	A235	6,754,212	06/22/2004	Terada et al.	
	A236	6,801,509	10/05/2004	Chuah et al.	
	A237	6,804,783	10/12/2004	Wesinger, Jr. et al.	
	A238	6,829,242	12/07/2004	Davison et al.	
	A239	6,834,271	12/21/2004	Hodgson et al.	
	A240	6,917,600	07/12/2005	Chuah et al.	
	A241	7,028,182	04/11/2006	Killcommons	
	A242	7,065,784	06/20/2006	Hopman et al.	
	A243	7,100,195	08/29/2006	Underwood	
	A244	7,103,770	09/05/2006	Conrath	
	A245	7,203,190	04/10/2007	Ruban et al.	
	A246	7,249,377	07/24/2007	Lita et al.	
	A247	7,307,990	12/11/2007	Rosen et al.	
	A248	6,701,437	03/03/2004	Hoke et al.	
	A249	4,405,829	09/20/1983	Rivest	
	A250	6,502,135	12/31/2002	Munger	
	A251	6,449,657	09/10/2002	Stanbach	
	A252	6,546,003	04/08/2003	Farris	
	A253	6,430,176	08/06/02	Christie	
	A254	6,930,998	08/16/2005	Sylvain	
	A255	6,065,049	05/16/2000	Beser et al.	
	A256	5,412,730	05/02/1995	Jones	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

/Krisna Lim/ 07/01/2014

	A257	7,669,049	02/23/2010	Wang et al.	
	A258	4,912,762	03/27/1990	Lee et al.	
	A258	7,275,113	09/25/2007	Araujo	
	A259	6,367,009	04/2002	Davis et al.	

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
	B25	US2002/0006132	01/17/2002	Chuah et al.,	
	B26	US2003/0005132	01/2003	Nguyen et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3 -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
	C29	JP 10-126440	05-15-1998	Hitachi Ltd.		English Abstract	
	C30	JP 11-355272	12-24-1999	Lucent Technol Inc.		English Abstract	
	C31	JP 11-355271	12-24-1999	Lucent Technol Inc.		English Abstract	
	C32	JP 11-261704	09-24-1999	Fujitsu Ltd.		English Abstract	
	C33	JP 10-70576	03-10-1998	Kokusai Denshin Denwa Co. Ltd.		English Abstract	
	C34	GB 2316841	03-04-1998	Kubota Ayumu et al.		English Abstract	
	C35	JP 09-266475	10-07-1997	Hitachi Ltd.		English Abstract	
	C36	JP 10-32610	02-03-1998	NEC Corp.		English Abstract	
	C37	WO 0014938	03-2000	Baehr et al.			
	C38	JP 09-275404	10/21/1997	Nippon Telegr & Teleph Corp.		English Abstract	
	C39	JP 11-167536	06/22/1999	Sun Microsyst Inc.		English Abstract	

07/01/2014

/Krisna Lim/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

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.	
	D1416	Request for Inter Partes Reexamination of Patent Number 7,490,151 filed on July 25, 2011, Requester Apple Inc. – Exhibit E3: Declaration of James Chester, 13 pages (2011)	
	D1417	Request for Inter Partes Reexamination of Patent Number 7,490,151 filed on July 25, 2011, Requester Apple Inc. – Exhibit A: Curriculum Vitae of James Chester, 4 pages	
	D1418	Request for Inter Partes Reexamination of Patent Number 7,490,151 filed on July 25, 2011, Requester Apple Inc. – Exhibit E1: Declaration of Chris Hopen, 5 pages	
	D1419	Request for Inter Partes Reexamination of Patent Number 7,490,151 filed on July 25, 2011, Requester Apple Inc. – Exhibit E2: Declaration of Michael Fratto, 51 pages (2011)	
	D1420	Request for Inter Partes Reexamination of Patent Number 7,490,151 filed on July 25, 2011, Requester Apple Inc. – Exhibit E: to Michael Fratto's Declaration, Fratto, "Aventail VPN 2.5: Not Your Father's Socks," Network Computing, Vol. 8, No. 18 (October 1, 1997), 3 pages	
	D1421	Request for Inter Partes Reexamination of Patent Number 7,490,151 filed on July 25, 2011, Requester Apple Inc. – Exhibit F: to Michael Fratto's Declaration, Fratto, "Footloose and Fancy Free with Three Socks 5-Based Proxy Servers," Network Computing, Vol. 9, Issue 11, 5 pages (June 15, 1998)	
	D1422	Request for Inter Partes Reexamination of Patent Number 7,490,151 filed on July 25, 2011, Requester Apple Inc. – Exhibit H: to Michael Fratto's Declaration, PR Newswire, "Aventail Ships Directory-enabled Extranet Solution; Aventail Extranet Center v3.1 Available at www.aventail.com." (August 9, 1998), 4 pages	
	D1423	Request for Inter Partes Reexamination of Patent Number 7,490,151 filed on July 25, 2011, Requester Apple Inc. – Exhibit I: to Michael Fratto's Declaration, "Intranet Applications: Briefs," Network World, at page 55 (October 19, 1998), 2 pages	
	D1424	Request for Inter Partes Reexamination of Patent Number 6,502,135 filed on July 11, 2011, Requester Apple Inc. – Exhibit E1: Declaration of Chris Hopen, 5 pages (2011)	
	D1425	Request for Inter Partes Reexamination of Patent Number 6,502,135 filed on July 11, 2011, Requester Apple Inc. – Exhibit E2: Declaration of Michael Fratto, 50 pages	
	D1426	Request for Inter Partes Reexamination of Patent Number 6,502,135 filed on July 11, 2011, Requester Apple Inc. – Exhibit E3: Declaration of James Chester, 13 pages	
	D1427	Request for Inter Partes Reexamination of Patent Number 7,921,211 filed on February 16, 2011, Requester Cisco Systems., - Original Petition to Request Inter Partes Reexamination, 40 pages	
	D1428	Request for Inter Partes Reexamination of Patent Number 8,051,181 filed on March 28, 2012, Requester Apple Inc. – Exhibit C2: Claim Chart – '181 Relative to Mattaway, 9 pages	
	D1429	Request for Inter Partes Reexamination of Patent Number 8,051,181 filed on March 28, 2012, Requester Apple Inc. – Exhibit C6: Claim Chart - '181 Relative to Johnson, 10 pages	
	D1430	Request for Inter Partes Reexamination of Patent Number 8,051,181 filed on March 28, 2012, Requester Apple Inc. – Exhibit C1: Claim Chart '181 Relative to Beser, 9 pages	
	D1431	Request for Inter Partes Reexamination of Patent Number 8,051,181 filed on March 28, 2012, Requester Apple Inc. – Exhibit C3: Claim Chart - '181 Relative to Lendenmann, 9 pages	
	D1432	Request for Inter Partes Reexamination of Patent Number 8,051,181 filed on March 28, 2012, Requester Apple Inc. – Exhibit C4: Claim Chart - '181 Relative to Provino, 9 pages	
	D1433	Request for Inter Partes Reexamination of Patent Number 8,051,181 filed on March 28, 2012, Requester Apple Inc. – Exhibit C5: Claim Chart – '181 Relative to H.323, 9 pages	
	D1434	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Petition for Inter Partes Review, 67 pages	

/Krisna Lim/ 07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1435	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1003: Declaration of Michael Fratto Regarding U.S. Patent Number 6,502,135, 195 pages (2013)	
	D1436	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1004: Fratto CV, 3 pages	
	D1437	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1005: Declaration of Chris Hopen Regarding Prior Art and U.S. Patent Number 6,502,135, 25 pages (2013)	
	D1438	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1006: Declaration of James Chester, 26 pages (2013)	
	D1439	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1019: Tittel, E., et al., Windows NT Server 4 for Dummies, Ch. 12, pp. 191-210 (1999)	
	D1440	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1020: Microsoft Windows 98 ResourceKit, 114 pages (1998)	
	D1441	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1024: Ole, "The Internet Protocol Journal, 1(2):1-48 (1998)	
	D1442	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1029: Rescorla, E., et al., RFC 2660, "The Secure HyperText Transfer Protocol," 45 pages (August 1999)	
	D1443	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1030: Lloyd, PPP Authentication Protocols, 15 pages (1992)	
	D1444	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1032: Dierks, "The TLS Protocol Version 1.0," 75 pages (1999)	
	D1445	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1040: Adams, C., et al., RFC 2510, "Internet X.509 Public Key Infrastructure Certificate Management Protocols," 68 pages (March 1999)	
	D1446	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1042: Record of Publication Ex:1015 on IEEE, 2 pages (1996)	
	D1447	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1043: Record of Publication of Reed (Ex. 1015) on ACM Digital Library, 2 pages (1996)	
	D1448	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1044: Record of Publication Ex:1015 on 12th ACSAC, 4 pages (1996)	
	D1449	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1045: Memorandum Opinion dated 7/30/09, 35 pages	
	D1450	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1047: Defendant's Responsive Claim Construction Brief, 37 pages (2011)	
	D1451	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1049: Memorandum Opinion and Order dated April 25, 2012, 31 pages	
	D1452	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1051: Nieh Declaration, 8 pages (2010)	
	D1453	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1057: CV Chris Hopen, 1 page	
	D1454	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1061: Network World Article, 1 page (1998)	

/Krisna Lim/ 07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1455	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1063: Malkin, G., RFC 2453, "RIP Version 2," 37 pages (November 1998)	
	D1456	IPR2013-00348; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1064:, J Moy, OSPF Version 2, 244 pages, (1998)	
	D1457	IPR2013-00349; Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Petition for Inter Partes Review, 73 pages	
	D1458	IPR2013-00349 Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1003: Declaration of Michael Fratto Regarding U.S. Patent Number 6,502,135, 256 pages (2013)	
	D1459	IPR2013-00349 Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1005: Declaration of Chris Hopen Regarding Prior Art and U.S. Patent Number 6,502,135, 25 pages (2013)	
	D1460	IPR2013-00349 Inter Partes Review of Patent Number 6,502,135 filed on June 12, 2013, Petitioner Apple Inc., – Exhibit 1006: Declaration of James Chester, 26 pages (2013)	
	D1461	IPR2013-00354; Inter Partes Review of Patent Number 7,490,151 filed on June 17, 2013, Petitioner Apple Inc., – Petition for Inter Partes Review, 73 pages	
	D1462	IPR2013-00354; Inter Partes Review of Patent Number 7,490,151 filed on June 14, 2013, Petitioner Apple Inc., – Exhibit 1003: Declaration of Michael Fratto Regarding U.S. Patent No. 7,490,151, 322 pages (2013)	
	D1463	IPR2013-00354; Inter Partes Review of Patent Number 7,490,151 filed on June 14, 2013, Petitioner Apple Inc., – Exhibit 1005: Declaration of Chris Hopen Regarding Prior Art and U.S. Patent No.: 7,490,151, 23 pages (2013)	
	D1464	IPR2013-00354; Inter Partes Review of Patent Number 7,490,151 filed on June 14, 2013, Petitioner Apple Inc., – Exhibit 1006: Declaration of James Chester, 26 pages (2013)	
	D1465	IPR2013-00354; Inter Partes Review of Patent Number 7,490,151 filed on June 14, 2013, Petitioner Apple Inc., – Exhibit 1048: VirnetX, Inc., Inc. vs. Cisco Systems, Inc., et al., VirnetX Reply Claim Construction Brief of December 19, 2011, 13 pages	
	D1466	IPR2013-00375; Inter Partes Review of Patent Number 6,502,135 filed on June 23, 2013, Petitioner New Bay Capital, LLC., – Petition for Inter Partes Review of Patent No. 6,502,135	
	D1467	IPR2013-00375; Inter Partes Review of Patent Number 6,502,135 filed on June 23, 2013, Petitioner New Bay Capital, LLC., – Exhibit 1002: The 1996 Symposium on Network and Distributed Systems Security (SNDSS'96), Hypermedia Proceedings, Slides, and Summary Report, 57 pages (1996)	
	D1468	IPR2013-00375; Inter Partes Review of Patent Number 6,502,135 filed on June 23, 2013, Petitioner New Bay Capital, LLC., – Exhibit 1005: Windows Sockets, An Open Interface for Network Programming under Microsoft Windows, Version 1.1, 124 pages (1993)	
	D1469	IPR2013-00375; Inter Partes Review of Patent Number 6,502,135 filed on June 23, 2013, Petitioner New Bay Capital, LLC., – Exhibit 1006: eCos Reference Manual, Chapter 38. TCP/IP Library Reference, downloaded from Http://www.ecos.sourceware.org/docs, 3 pages (March 13, 1997)	
	D1470	IPR2013-00375; Inter Partes Review of Patent Number 6,502,135 filed on June 23, 2013, Petitioner New Bay Capital, LLC., – Exhibit 1009: Declaration of Russell Housley Regarding U.S. Patent Number 6,502,135, 105 pages (June 22, 2003)	
	D1471	IPR2013-00375; Inter Partes Review of Patent Number 6,502,135 filed on June 23, 2013, Petitioner New Bay Capital, LLC., – Exhibit 1012: VirnetX Inc., vs. Apple; Transcript of Pretrial Conference on October 18, 2012, 216 pages	
	D1472	IPR2013-00375; Inter Partes Review of Patent Number 6,502,135 filed on June 23, 2013, Petitioner New Bay Capital, LLC., – Exhibit 1013: VirnetX, Inc., vs. Apple: Trial Transcript (Morning Session) of October 31, 2012, 128 pages	

/Krisna Lim/ 07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1473	IPR2013-00375; Inter Partes Review of Patent Number 6,502,135 filed on June 23, 2013, Petitioner New Bay Capital, LLC., – Exhibit 1014: Trial Transcript (Morning Session) of November 1, 2012, 146 pages	
	D1474	IPR2013-00375; Inter Partes Review of Patent Number 6,502,135 filed on June 23, 2013, Petitioner New Bay Capital, LLC., – Exhibit 1015: VirnetX Inc., vs. Apple; Memorandum Opinion and Order dated February 26, 2013, 47 pages	
	D1475	IPR2013-00375; Inter Partes Review of Patent Number 6,502,135 filed on June 23, 2013, Petitioner New Bay Capital, LLC., – Exhibit 1018: Virnetx Reply Claim Construction, 13 pages (2011)	
	D1476	IPR2013-00376; Inter Partes Review of Patent Number 7,490,151 filed on June 23, 2013, Petitioner New Bay Capital, LLC. – Petition for Inter Partes Review of U.S. Patent Number 7,490,151, 68 pages	
	D1477	IPR2013-00378; Inter Partes Review of Patent Number 7,921,211 filed on June 23, 2013, Petitioner New Bay Capital, LLC., – Petition for Inter Partes Review of U.S Patent No. 7,921,211	
	D1478	IPR2013-00378; Inter Partes Review of Patent Number 7,921,211 filed on June 23, 2013, Petitioner New Bay Capital, LLC., – Exhibit 1004: Declaration of Russell Housley Regarding U.S. Patent Number 7,418,504, 98 pages (2013)	
	D1479	IPR2013-00378; Inter Partes Review of Patent Number 7,921,211 filed on June 23, 2013, Petitioner New Bay Capital, LLC., – Exhibit 1009: VirnetX, Inc., vs. Mitel Networks Corp., et al., VirnetX Opening Claim Construction Brief, 28 pages (2012)	
	D1480	IPR2013-00378; Inter Partes Review of Patent Number 7,921,211 filed on June 23, 2013, Petitioner New Bay Capital, LLC., – Exhibit 1010: The American Heritage Dictionary of the English Language, Third Edition, 4 pages (1996)	
	D1481	IPR2013-00393; Inter Partes Review of Patent Number 7,418,504 filed on July 1, 2013, Petitioner Apple Inc., – Petition for Inter Partes Review of US Patent No 7,418,504, 62 pages	
	D1482	IPR2013-00393; Inter Partes Review of Patent Number 7,418,504 filed on July 1, 2013, Petitioner Apple Inc., – Exhibit 1003: Declaration of Michael Fratto, 182 pages (2013)	
	D1483	IPR2013-00393; Inter Partes Review of Patent Number 7,418,504 filed on July 1, 2013, Petitioner Apple Inc., – Exhibit 1005: Declaration of Chris Hopen, 25 pages (2013)	
	D1484	IPR2013-00393; Inter Partes Review of Patent Number 7,418,504 filed on July 1, 2013, Petitioner Apple Inc., – Exhibit 1006: Declaration of James Chester , 26 pages (2013)	
	D1485	IPR2013-00393; Inter Partes Review of Patent Number 7,418,504 filed on July 1, 2013, Petitioner Apple Inc., – Exhibit 1065: Yeager, Web Server Technology, 54 pages (1996)	
	D1486	IPR2013-00393; Inter Partes Review of Patent Number 7,418,504 filed on July 1, 2013, Petitioner Apple Inc., – Exhibit 1066: Microsoft Intemet Explorer 5 Resource Kit, 21 pages (1999)	
	D1487	IPR2013-00393; Inter Partes Review of Patent Number 7,418,504 filed on July 1, 2013, Petitioner Apple Inc., – VirnetX Exhibit 2015: ITU-T Recommendation X.500, "Series Data Networks," 32 pages (2008)	
	D1488	IPR2013-00394; Inter Partes Review of Patent Number 7,418,504 filed on July 1, 2013, Petitioner Apple Inc., – Petition for Inter Partes Review of US Patent No 7,418,504, 73 pages	
	D1489	IPR2013-00394; Inter Partes Review of Patent Number 7,418,504 filed on July 1, 2013, Petitioner Apple Inc., - Exhibit 1003: Declaration of Michael Fratto, 203 pages (2013)	
	D1490	IPR2013-00394; Inter Partes Review of Patent Number 7,418,504 filed on July 1, 2013, Petitioner Apple Inc., - Exhibit 1005: Hopen Declaration, 25 pages (2013)	
	D1491	IPR2013-00394; Inter Partes Review of Patent Number 7,418,504 filed on July 1, 2013, Petitioner Apple Inc., - Exhibit 1006: Chester Declaration, 26 pages (2013)	
	D1492	IPR2013-00397; Inter Partes Review of Patent Number 7,921,211 filed on July 1, 2013, Petitioner Apple Inc., - Petition for Inter Partes Review, 63 pages (2013)	
	D1493	IPR2013-00397; Inter Partes Review of Patent Number 7,921,211 filed on July 1, 2013, Petitioner Apple Inc., - Exhibit 1003: Declaration of Michael Fratto, 184 pages (2013)	
	D1494	IPR2013-00397; Inter Partes Review of Patent Number 7,921,211 filed on July 1, 2013, Petitioner Apple Inc., - Exhibit 1005: Declaration of Chris Hopen, 25 pages (2013)	

/Krisna Lim/ 07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1495	IPR2013-00397; Inter Partes Review of Patent Number 7,921,211 filed on July 1, 2013, Petitioner Apple Inc., - Exhibit 1006: Declaration of James Chester, 26 pages (2013)	
	D1496	IPR2013-00398; Inter Partes Review of Patent Number 7,921,211 filed on July 1, 2013, Petitioner Apple Inc., Petition for Inter Partes Review, 74 pages	
	D1497	IPR2013-00398; Inter Partes Review of Patent Number 7,921,211 filed on July 1, 2013, Petitioner Apple Inc., Exhibit 1003: Declaration of Michael Fratto regarding Patent Number 7,921,211, 204 pages (2013)	
	D1498	IPR2013-00398; Inter Partes Review of Patent Number 7,921,211 filed on July 1, 2013, Petitioner Apple Inc., Exhibit 1005: Declaration of Chris Hopen, 25 pages (2013)	
	D1499	IPR2013-00398; Inter Partes Review of Patent Number 7,921,211 filed on July 1, 2013, Petitioner Apple Inc., Exhibit 1006: Declaration of James Chester, 26 pages (2013)	
	D1500	IPR2014-00176; Inter Partes Review of Patent Number 7,418,504 filed on November 20, 2013, Petitioner RPX Corporation; Petition for Inter Partes Review, 60 pages	
	D1501	IPR2014-00176; Inter Partes Review of Patent Number 7,418,504 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1003; Declaration of Michael Fratto Regarding U.S. Patent Number 7,418,504, 242 pages (2013)	
	D1502	IPR2014-00176; Inter Partes Review of Patent Number 7,418,504 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1005; Declaration of Christ Hopen, 25 pages (2013)	
	D1503	IPR2014-00176; Inter Partes Review of Patent Number 7,418,504 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1006; Declaration of James Chester, 26 pages (2013)	
	D1504	IPR2014-00174; Inter Partes Review of Patent Number 7,418,504 filed on November 20, 2013, Petitioner RPX Corporation; Petition for Inter Partes Review, 60 pages	
	D1505	IPR2014-00174; Inter Partes Review of Patent Number 7,418,504 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1003: Declaration of Michael Fratto Regarding U.S. Patent Number 7,921,211, 242 pages (2013)	
	D1506	IPR2014-00174; Inter Partes Review of Patent Number 7,418,504 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1005: Declaration of Chris Hopen, 25 pages (2013)	
	D1507	IPR2014-00174; Inter Partes Review of Patent Number 7,418,504 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1006: Declaration of James Chester, 26 pages (2013)	
	D1508	IPR2014-00172; Inter Partes Review of Patent Number 6,502,135 filed on November 20, 2013, Petitioner RPX Corporation; Petition for Inter Partes Review, 67 pages	
	D1509	IPR2014-00172; Inter Partes Review of Patent Number 6,502,135 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1003:Declaration of Michael Fratto Regarding U.S. Patent Number 6,502,135, 196 pages (2013)	
	D1510	IPR2014-00172; Inter Partes Review of Patent Number 6,502,135 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1005: Declaration of Chris Hopen Regarding Prior Art and U.S. Patent Number 6,502,135, 25 pages (2013)	
	D1511	IPR2014-00172; Inter Partes Review of Patent Number 6,502,135 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1006: Declaration of James Chester, 26 pages (2013)	
	D1512	IPR2014-00171; Inter Partes Review of Patent Number 6,502,135 filed on November 20, 2013, Petitioner RPX Corporation; Petition for Inter Partes Review, 73 pages	
	D1513	IPR2014-00171; Inter Partes Review of Patent Number 6,502,135 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1003:Declaration of Michael Fratto Regarding U.S. Patent Number 6,502,135, 286 pages (2013)	
	D1514	IPR2014-00171; Inter Partes Review of Patent Number 6,502,135 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1005: Declaration of Chris Hopen Regarding Prior Art and U.S. Patent Number 6,502,135, 25 pages (2013)	
	D1515	IPR2014-00171; Inter Partes Review of Patent Number 6,502,135 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1006: Declaration of James Chester, 26 pages (2013)	
	D1516	IPR2014-00173; Inter Partes Review of Patent Number 7,490,151 filed on November 20, 2013, Petitioner RPX Corporation; Petition for Inter Partes Review, 72 pages	

/Krisna Lim/ 07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1517	IPR2014-00173; Inter Partes Review of Patent Number 7,490,151 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1003:Declaration of Michael Fratto Regarding U.S. Patent Number 6,502,135, 352 pages (2013)	
	D1518	IPR2014-00173; Inter Partes Review of Patent Number 7,490,151 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1005: Declaration of Chris Hopen Regarding Prior Art and U.S. Patent Number 7,490,151, 23 pages (2013)	
	D1519	IPR2014-00173; Inter Partes Review of Patent Number 7,490,151 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1006: Declaration of James Chester, 26 pages (2013)	
	D1520	IPR2014-00175; Inter Partes Review of Patent Number 7,921,211 filed on November 20, 2013, Petitioner RPX Corporation; Petition for Inter Partes Review, 66 pages	
	D1521	IPR2014-00175; Inter Partes Review of Patent Number 7,921,211 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1003:Declaration of Michael Fratto Regarding U.S. Patent Number 6,502,135, 209 pages (2013)	
	D1522	IPR2014-00175; Inter Partes Review of Patent Number 7,921,211 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1005: Declaration of Chris Hopen Regarding Prior Art and U.S. Patent Number 7,490,151, 25 pages (2013)	
	D1523	IPR2014-00175; Inter Partes Review of Patent Number 7,921,211 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1006: Declaration of James Chester, 26 pages (2013)	
	D1524	IPR2014-00177; Inter Partes Review of Patent Number 7,418,504 filed on November 20, 2013, Petitioner RPX Corporation; Petition for Inter Partes Review, 63 pages	
	D1525	IPR2014-00177; Inter Partes Review of Patent Number 7,418,504 filed on November 20, 2013, Petitioner RPX Corporation; Exhibit 1003:Declaration of Michael Fratto Regarding U.S. Patent Number 6,502,135, 208 pages (2013)	
	D1526	IPR2014-00177; Inter Partes Review of Patent Number 7,418,504 filed on November 20, 2013, Apple Inc.; Exhibit 1005: Declaration of Chris Hopen Regarding Prior Art and U.S. Patent Number 7,490,151, 25 pages (2013)	
	D1527	IPR2014-00177; Inter Partes Review of Patent Number 7,418,504 filed on November 20, 2013, Apple Inc.; Exhibit 1006: Declaration of James Chester, 26 pages (2013)	
	D1528	IPR2014-00237; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc.; Petition for Inter Partes Review, 72 pages	
	D1529	IPR2014-00237; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc.; Exhibit 1003: Declaration of Michael Fratto Regarding U.S. Patent Number 8,504,697, 201 pages	
	D1530	IPR2014-00237; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc.; Exhibit 1015: Wedlund et al., "Mobility Support Using SIP,"pages 76-82 (1999)	
	D1531	IPR2014-00237; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Exhibit 1013: Schulzrinne et al., A Transport Protocol for Real-Time Applications, RFC 1889, 75 pages (1996)	
	D1532	IPR2014-00237; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Exhibit 1014: Handley et al., Session Description Protocol, RFC 2327,42 pages (1998)	
	D1533	IPR2014-00237; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Exhibit 1066: WAP Architecture Version 30, 20 pages (1998)	
	D1534	IPR2014-00237; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Exhibit 1067: World Wide Web Consortium and Wirelss Application Protocol Forum Establish Formal Liaison Relationship, 3 pages (1999)	
	D1535	IPR2014-00237; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Exhibit 1068: Data Over Cable Interface Specifications, 189 pages (1997)	
	D1536	IPR2014-00237; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Exhibit 1069: Nikolich, Cable Modems Deliver Fast Net Access, LexisNexis, 2 pages (1999)	
	D1537	IPR2014-00237; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Exhibit 1070: Duffy, Cabletron Enters Cable Modem Fray, LexisNexis, 2 pages (1998)	

/Krisna Lim/ 07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1538	IPR2014-00237; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Exhibit 1071: How it Works: Cable Modems, 2 pages (1999)	
	D1539	IPR2014-00237; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Exhibit 1072: Microsoft Press, Microsoft Computer Dictionary Fourth Edition, 9 pages (1999)	
	D1540	IPR2014-00237; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Exhibit 1075: IBM Session Initiation Protocol, 4 pages (2013)	
	D1541	IPR2014-00237; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Exhibit 1079: Shorter Oxford English Dictionary on Historical Principles, Fifth Edition, Volume 1 A-M, 3 pages (2002)	
	D1542	IPR2014-00238; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Petition for Inter Partes Review, 72 pages	
	D1543	IPR2014-00238; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Exhibit 1003: Declaration of Michael Fratto Regarding U.S. Patent Number 8,504,697, 240 pages (2013)	
	D1544	IPR2014-00238; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Exhibit 1005: Declaration of Chris Hopen Regarding Prior Art and U.S. Patent Number 7,490,151,23 pages (2013)	
	D1545	IPR2014-00238; Inter Partes Review of Patent Number 8,504,697 filed on November 20, 2013, Apple Inc; Exhibit 1006: Declaration of James Chester, 26 pages (2013)	
	D1546	IPR2014-00401; Inter Partes Review of Patent Number 7,188,180 filed on February 4, 2014, Petitioner Microsoft Corporation., – Petition for Inter Partes Review, 62 pages	
	D1547	IPR2014-00401; Inter Partes Review of Patent Number 7,188,180 filed on February 4, 2014, Petitioner Microsoft Corporation., - Exhibit 1005: Guillen et al., "An Architecture for Virtual Circuit/QoS Routing," Brussels University, 8 pages (1993)	
	D1548	IPR2014-00401; Inter Partes Review of Patent Number 7,188,180 filed on February 4, 2014, Petitioner Microsoft Corporation., - Exhibit 1006: Kosiur, "Building and Managing Virtual Private Networks," Wiley Computer Publishing, ISBN: 0471295264 (1998)	
	D1549	IPR2014-00401; Inter Partes Review of Patent Number 7,188,180 filed on February 4, 2014, Petitioner Microsoft Corporation., - Exhibit 1011: Guerin Declaration for 180 Patent (Provino) dated January 10, 2014	
	D1550	IPR2014-00401; Inter Partes Review of Patent Number 7,188,180 filed on February 4, 2014, Petitioner Microsoft Corporation., - Exhibit 1015: Redacted Settlement Agreement dated 5/14/2010	
	D1551	IPR2014-00403; Inter Partes Review of Patent Number 7,987,274 filed on February 4, 2014, Petitioner Microsoft Corporation., – Petition for Inter Partes Review, 58 pages	
	D1552	IPR2014-00403; Inter Partes Review of Patent Number 7,987,274 filed on February 4, 2014, Petitioner Microsoft Corporation., - Exhibit 1002: Excerpts from the Prosecution History of USP 7,987,274 filed 5/21/2013.	
	D1553	IPR2014-00404; Inter Partes Review of Patent Number 7,987,274 filed on February 4, 2014, Petitioner Microsoft Corporation., – Petition for Inter Partes Review, 58 pages	
	D1554	IPR2014-00404; Inter Partes Review of Patent Number 7,987,274 filed on February 4, 2014, Petitioner Microsoft Corporation., – Exhibit 1002: Excerpts from the Prosecution History of USP 7,987,274 dated 4/22/2013	
	D1555	IPR2014-00405; Inter Partes Review of Patent Number 7,987,274 filed on February 4, 2014, Petitioner Microsoft Corporation., – Petition for Inter Partes Review, 66 pages	
	D1556	IPR2014-00405; Inter Partes Review of Patent Number 7,987,274 filed on February 4, 2014, Petitioner Microsoft Corporation., - Exhibit 1012: Order of Dismissal dated 6/10/2010	
	D1557	IPR2014-00405; Inter Partes Review of Patent Number 7,987,274 filed on February 4, 2014, Petitioner Microsoft Corporation., - Exhibit 1013: Order of Dismissal dated 5/25/2010	
	D1558	IPR2014-00405; Inter Partes Review of Patent Number 7,987,274 filed on February 4, 2014, Petitioner Microsoft Corporation., Exhibit 1024: Excerpt from Prosecution History of Reexam 95/001,972	

/Krisna Lim/ 07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1559	VirnetX v. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013, 43 pages	
	D1560	VirnetX v. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 37: SecureConnect vs. Claims of the '151 Patent, 4 pages	
	D1561	VirnetX v. Microsoft, Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 41: SFS-HTTP vs. Claims of the '151 Patent, 10 pages	
	D1562	VirnetX v. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 48: U.S. '132 vs. Claims of the '151 Patent, 15 pages	
	D1563	VirnetX v. Microsoft, Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 55: B&M VPNs vs. Claims of the '151 Patent, 12 pages	
	D1564	VirnetX v. Microsoft, Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 59: BorderManager vs. Claims of the '151 Patent, 18 pages	
	D1565	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 79: Valencia (019) vs. Claims of the '274 Patent, 12 pages	
	D1566	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 85: U.S. '748 vs. Claims of the '151 Patent, 8 pages	
	D1567	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 99: Araujo vs. Claims of the '135 Patent, 19 pages	
	D1568	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 100: Araujo vs. Claims of the "151 Patent, 8 pages	
	D1569	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 101: NetMeeting vs. Claims of the '135 Patent, 81 pages	
	D1570	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 102: NetMeeting vs. Claims of the '151 Patent, 53 pages	
	D1571	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 103: NetMeeting vs. Claims of the '180 Patent, 35 pages	
	D1572	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 104: NetMeeting vs. Claims of the '211 Patent, 47 pages	
	D1573	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 105: NetMeeting vs. Claims of the '274 Patent, 26 pages	
	D1574	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 106: NetMeeting vs. Claims of the '504 Patent, 48 pages	
	D1575	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 107: EverLink vs. Claims of the '151 Patent, 39 pages	
	D1576	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 108: Special Anthology vs. Claims of the '135 Patent, 4 pages	
	D1577	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 109: Gauntlet for IRIX vs. Claims of the '135 Patent, 62 pages	
	D1578	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 110: Gauntlet for IRIX vs. Claims of the '211 Patent, 111 pages	
	D1579	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 111: Gauntlet for IRIX vs. Claims of the '504 Patent, 119 pages	
	D1580	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 112: Gauntlet System vs. Claims of the '135 Patent, 24 pages	
	D1581	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 113: Gauntlet System vs. Claims of the '151 Patent, 23 pages	
	D1582	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 108: Gauntlet System vs. Claims of the '180 Patent, 36 pages	
	D1583	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 115: Gauntlet System vs. Claims of the '211 Patent, 67 pages	
	D1584	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 116: Gauntlet Systems vs. Claims of the '504 Patent, 69 pages	
	D1585	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 117: Gauntlet Systems vs. Claims of the '274 Patent, 16 pages	

/Krisna Lim/ 07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1586	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 123: IntraPort System vs. Claims of the '274 Patent, 24 pages	
	D1587	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 129: Overview vs. Claims of the '274 Patent, 12 pages	
	D1588	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 135: Schulzrinne vs. Claims of the '274 Patent, 14 pages	
	D1589	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 141: Solana vs. Claims of the '274 Patent, 17 pages	
	D1590	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 147: Atkinson vs. Claims of the '274 Patent, 15 pages	
	D1591	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 153: Marino vs. Claims of the '274 Patent, 11 pages	
	D1592	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 159: Valencia (213) vs. Claims of the '274 Patent, 13 pages	
	D1593	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 166: Davison vs. Claims of the '274 Patent, 11 pages	
	D1594	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 170: AutoSOCKS vs. Claims of the '274 Patent, 14 pages	
	D1595	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 174: Aventail Connect 3.01/2.51 vs. Claims of the '274 Patent, 17 pages	
	D1596	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 176: Aventail Connect 3.1/2.6 Administrator's Guide("Aventail Connect") vs. Claims of the '211 Patent, 56 pages	
	D1597	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 179: Aventail Connect 3.1/2.6 vs. Claims of the '274 Patent, 19 pages	
	D1598	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 183: BinGO! User's Guide/Extended Features Reference vs. Claims of the '274 Patent, 26 pages	
	D1599	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 210: Cisco's Prior Art Systems vs. Claims of the '274 Patent, 19 pages	
	D1600	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 213: Cisco's Prior Art PIX System vs. Claims of the '151 Patent, 37 pages	
	D1601	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 214: Cisco's Prior Art PIX System vs. Claims of the '211 Patent, 104 pages	
	D1602	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 244: Understanding OSF DCE 1.1 for AIX and OS/2 (APP_VX0556531-804) vs. Claims of the '274 Patent, 26 pages	
	D1603	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 228: Abadi vs. Claims of the '135 Patent, 12 pages	
	D1604	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 229: Abadi vs. Claims of the '180 Patent, 16 pages	
	D1605	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 230: Abadi vs. Claims of the '151 Patent, 10 pages	
	D1606	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 231: Abadi vs. Claims of the '274 Patent, 11 pages	
	D1607	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 237: Kiuchi vs. Claims of the '274 Patent, 30 pages	
	D1608	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 243: Aziz vs. Claims of the '274 Patent, 37 pages	
	D1609	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 248: RFC 2543 vs. Claims of the '180 Patent, 48 pages	
	D1610	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 249: RFC 2543 vs. Claims of the '274 Patent, 28 pages	

/Krisna Lim/ 07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1611	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 252: Wesinger vs. Claims of the '180 Patent, 42 pages	
	D1612	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 253: Wesinger vs. Claims of the '274 Patent, 23 pages	
	D1613	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 257: Provino vs. Claims of the '180 Patent, 17 pages	
	D1614	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 258: U.S. Patent Number 6,557,037 vs. Claims of the '504 Patent, 17 pages	
	D1615	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 259: Provino vs. Claims of the '151 Patent, 13 pages	
	D1616	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 261: Provino vs. Claims of the '274 Patent, 15 pages	
	D1617	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 262: NT4 System vs. Claims of the '135 Patent, 22 pages	
	D1618	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 263: NT4 System vs. Claims of the '151 Patent, 12 pages	
	D1619	VirnetX vs. Microsoft; Defendant's Preliminary Invalidity Contentions dated 11/14/2013; Exhibit 264: EverLink vs. Claims of the '274 Patent, 38 pages	
	D1620	New Version of Windows 98 Improves the Business of Running a Home; Windows 98 Second Edition Makes it Easier for Families to Connect, June 10, 1999	
	D1621	Research Advances in Database and Information Systems Security, Kluwer Academic Publishers, July 25-28 (1999)	
	D1622	Barkley et al., "Role Based Access Control for the World Wide Web," Abstract, pages 1-11, April 8 (1997)	
	D1623	Abadi et al., "Secure Web Tunneling," Computer Networks and ISDN Systems, 30:531-539 (1998)	
	D1624	Communications and Multimedia Security II; Proceedings of the IFIP TC6/TC11 International Conference on Communications and Multimedia Security at Essen, Germany, September 23-24 (1996)	
	D1625	IEEE Computer Society, Seventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE '98); June 17-19 (1998)	
	D1626	Kahan, "WDAI: A Simple World Wide Web Distributed Authorization Infrastructure," Computer Networks, 31:1599-1609 (1999)	
	D1627	Norifusa, "Internet Security: Difficulties and Solutions," International Journal of Medical, 49:69-74 (1998)	
	D1628	Molva, "Internet Security Architecture," 31:787-804 (1999)	
	D1629	Ellermann, "IPv6 and Firewalls," June 1996	
	D1630	Herscovitz, "Secure Virtual Private Networks: The Future of Data Communications," International Journal of Network Management, 9:213-220 (1999)	
	D1631	Cheswick et al., "A DNS Filter and Switch for Packet-Filtering Gateways," Proceedings of the Sixth USENIX UNIX Security Symposium, 1996	
	D1632	Farrow, "How DNS Can Divulge Sensitive Information," Network Magazine, 14(3):72 (1999)	
	D1633	Greenwald et al., "Designing an Academic Firewall: Policy, Practice, and Experience with SURF," Proceedings of the SNDSS, 1996	
	D1634	Collins, "Designing Secure Intranets," Computing & Control Engineering Journal, pages 185-192, 1998	
	D1635	Lioy et al., "DNS Security," Terena Networking Conference, pages 1-13, May 22-25 (2000)	
	D1636	Davidowicz, "Domain Name System (DNS) Security," pages 1-22, (1999)	
	D1637	Gilmore et al., "Secure Remote Access to an Internal Web Server," IEEE Network, pages 31-37 (1999)	

/Krisna Lim/ 07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1638	Using NETBuilder Family Software, Version 11.0, Published March 1998, http://www.3com.com/	
	D1639	AccessBuilder 2000/4000/5000 Server Configuration Guide, Software Version 7.0, Published April 1997, http://www.3com.com/	
	D1640	Apple Remote Access 3.0, Apple Remote Access Client and Apple Remote Access Personal Server User's Manual (1997)	
	D1641	Macaire et al., "A Personal Naming and Directory Service for Mobile Internet Users," USENIX Workshop on Smartcard Technology, May 10-11 (1999)	
	D1642	Sidewinder Network Gateway Security, Administration Guide Version 7.0, Secure Computing Corporation, 812 pages (2007)	
	D1643	Zao et al., "Domain Based Internet Security Policy Management," pages 41-53 (1999)	
	D1644	Aventail and Spyrus Join Forces to Deliver High-Assurance Extranet Security Solutions for the Enterprise, Business Wire, May 12, 1999	
	D1645	Aventail Ships Directory-Enabled Extranet Solution; Aventail Extranet Center V3.1 Available at www.aventail.com, Business Wire, August 9, 1999	
	D1646	Mooi Choo Chuah et al., "Mobile Virtual Private Dial-Up Services," Bell Labs Technical Journal, (1999)	
	D1647	The Brick Extended Features Reference.Manual, 288 pages (1999)	
	D1648	Bianca/Brick Software Reference Manual, Version 2.3, 331 pages (1999)	
	D1649	Bianca/Brick Software Reference Manual, Version 2.4, (1999)	
	D1650	Novell BorderManager; Installation and Setup, Version 3.5, 162 pages (1999)	
	D1651	Broadband Forum Technical Support, Core Network Architecture Recommendations for Access to Legacy Data Networks Over ADSL, Issue 1.0, 24 pages (1999)	
	D1652	Cabletron Routing Software; Routing Protocols Reference Guide, Cabletron Systems (1999)	
	D1653	Cisco Systems, Virtual Private Networks (VPN), Internetworking Technical Overview, (1999)	
	D1654	Cisco Systems, Cisco Access Product Family, 16 pages (1996)	
	D1655	Cisco, MPLS Virtual Private Networks, (1999)	
	D1656	WEBDAV: Distributed Authoring and Versioning Presentation vs. Greg Stein, Adobe Technical Seminar Series, May, 1999	
	D1657	Valencia et al., "Layer Two Tunneling Protocol "LSTP"," Internet Draft (1998)	
	D1658	Patel, "Securing L2TP Using IPSEC," Internet Draft (1999)	
	D1659	Srisuresh, "Secure Remote Access with L2TP," Internet Draft (1999)	
	D1660	IBM Corporation, AS/400 TCP/IP Autoconfiguration DNS and DHCP Support, 457 pages (1998) available at http://www.redbooks.ibm.com	
	D1661	IBM Corporation, Inside the VPN Tunnel, IBM Technical Support, 23 pages (1999)	
	D1662	IBM Corporation, IBM Firewall for AS/400 V4R3: VPN and NAT Support, 361 pages (1999)	
	D1663	IBM Corporation, Software User's Guide, Version 3.2, (1998)	
	D1664	IBM Corporation, Software User's Guide Version 3.3, 678 pages (1999)	
	D1665	IBM Corporation, Using and Configuring Features, Version 3.2, 336 pages, (1998)	
	D1666	IBM Corporation, Software User's Guide, Version 3.4, 770 pages (1999)	
	D1667	IBM Corporation, A Comprehensive Guide to Virtual Private Networks, Volume I: IBM Firewall, Server and Client Solutions, 36 pages (1998) available at http://www.redbooks.ibm.com	

/Krisna Lim/ 07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1668	IBM Corporation, A Comprehensive Guide to Virtual Private Networks, Volume II: IBM Nways Router Solutions, 622 pages (1999) available at http://www.redbooks.ibm.com	
	D1669	IBM Corporation, A Comprehensive Guide to Virtual Private Networks, Volume III: Cross-Platform Key and Policy Management, 665 pages (1999) available at http://www.redbooks.ibm.com	
	D1670	Novell, BorderManager, Overview and Planning, Enterprise Edition 3, Version 3.5 (1999)	
	D1671	Zyxel Total Intemet Access Solution; User's Guide, Version 2.20 (1999)	
	D1672	Raptor Integrated Enterprise Network Security System V6.0; Raptor Firewall Reference Guide (1998)	
	D1673	Reynolds et al., "Assigned Numbers," RFC 1700 (1994)	
	D1674	Blake et al., "An Architecture for Differentiated Services," RFC 2475 (1998)	
	D1675	Aboba et al., "The Network Access Identifier," RFC 2486 (1999)	
	D1676	Rosen et al., "BGP/MPLS VPNs, RFC 2547 (1999)	
	D1677	Pall et al., "Microsoft Point-To-Point Encryption (MPPE) Protocol," RFC 3078 (2001)	
	D1678	Cisco Systems, Release Notes for the Cisco Secure VPN Client Versions 1.0/1.0a (1999)	
	D1679	Ascend Communications, Inc., SecureConnect Manager User's Guide (1998)	
	D1680	Kaminsky et al., "SFS-HTTP: Securing the Web with Self-Certifying URLs," (1999) available at http://www.pdos.lcs.mit.edu/"kaminsky/sfs-http.ps	
	D1681	Timestep Corporation, Understanding the IPSec Protocol Suite (1998)	
	D1682	Level One, Level One User Manual (1999)	
	D1683	Stein et al., "Writing Apache Modules with Perl and C," ISBN:1-56592-567, 746 pages (1999)	
	D1684	Shea, "L2TP Implementation and Operation," The Addison-Wesley Networking Basics Series (2000)	
	D1685	McCormack et al., "An Authentication Framework for Web Access to Remote Hosts," National Institute of Standards and Technology (1998)	
	D1686	Harney et al., "Group Key Management Protocol (GKMP) Architecture," RFC 2094 (1997)	
	D1687	Sijben et al., "Bridging the Gap to IP Telephony," Bell Labs Technical Journal (1998)	
	D1688	Hoffman, "SMTP Service Extension for Secure SMTP over TLS," RFC 2487 (1999)	
	D1689	Newman, "Using TLS with IMAP, POP3 and ACAP," RFC 2595 (1999)	
	D1690	Using Internet VPN to Bring Job Sites and Branch Offices Online, Nikkei Communications (1997)	
	D1691	ANX CEP Interconnection Options, Bellcore/ANXO, October 1, 1998	
	D1692	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Atkinson, "An Internetwork Authentication Architecture," Naval Research Laboratory, Center for High Assurance Computing Systems (8/5/93)	
	D1693	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Eastlake, Domain Name System Security Extensions, IETF DNS Security Working Group (December 1998), available at http://www.watersprins.org/pub/id/draft-ietf-dnssec-secext2-07.txt	
	D1694	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Goldschlag et al., "Privacy on the Internet," Naval Research Laboratory, Center for High Assurance Computer Systems (1997)	
	D1695	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Goldschlag et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK (May 1996)	

/Krisna Lim/

07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1696	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Goldschlag et al., "Onion Routing for Anonymous and Private Internet Connection," Naval Research Laboratory, Center for High Assurance Computer Systems (January 28, 1999)	
	D1697	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. M.G. Reed et al., "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA December 9-13 1996	
	D1698	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Macdonald et al., "PF_KEY key Management API, Version 2," Network Working Group, RFC 2367 (July 1998) ("RFC 2367")	
	D1699	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Onion Routing, "Investigation of Route Selection Algorithms," available at http://www.onion-router.net/Archives/Route/index.html ("Route Selection")	
	D1700	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Scott et al., Virtual Private Networks, O'Reilly and Associates, Inc., 2nd ed (Jan. 1999) ("Scott VPNs')	
	D1701	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Syverson et al., "Private Web Browsing," Naval Research Laboratory, Center for High Assurance Computer Systems (June 2, 1997) ("Syverson")	
	D1702	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. "IPSec Minutes From Montreal," IPSEC Working Group Meeting Notes, http://www.sandleman,ca/ipsec/1996/08/msg00018.html (June 1996)	
	D1703	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. "Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources," FirstVPN, (Jan 2000) ("First VPN Building a Microsoft VPN Publication")	
	D1704	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Publicly Available DNS-Related Correspondence dated September 7, 1993 to September 20, 1993 ("DNS-Related Correspondence")	
	D1705	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Assured Digital Incorporated Products ("ADI Products")	
	D1706	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. DNS SRV references (1996, 1998, 1999, 2000)	
	D1707	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. U.S. Patent Number 5,898,830 ("Wesinger '830 Patent")	
	D1708	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Global VPN ("GVPN") references (1999)	
	D1709	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Kaufman et al., Implementing IPsec: Making Security Work on VPNs, Intranets, and Extranets, (Copyright 1999) ("Implementing IPsec")	
	D1710	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Safe Surfing: How to Build a Secure World Wide Web Connection, IBM Int'l Technical Support Organization (March 1996) ("Safe Surfing")	
	D1711	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. U.S. Provision Patent Application No. 60/134,547 (filed May 17, 1999) ("Sheymov")	
	D1712	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Data Fellows F-Secure VPN ("F-Secure VPN+ Publication")	
	D1713	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. U.S. Pat. No. 5,950,195 ("Stockwell '195 Patent")	
	D1714	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. B. Patel et al., "DHCP Configuration of IPSEC Tunnel Mode," IPSEC Working Group, Internet Draft 02 (10/15/1999) ("Patel")	
	D1715	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. SSL VPNs ("SSL VPNs") references (1996, 1997, 1998)	
	D1716	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Gauntlet Firewall ("Gauntlet FW") references (1995, 1996, 1999)	
	D1717	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. U.S. Pat. No. 6,119,171 ("'171 patent")	
	D1718	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Caronni et al., U.S. Patent No. 5,822,434 October 13, 1998 (filed June 18, 1996) ("'434 patent)	

/Krisna Lim/

07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1719	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. RFC 2230 (November 1997) U.S. Patent No. 5,511,122 (April 23, 1996)	
	D1720	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Check Point FW as described in: Goncalves et al., Check Point Firewall -1 Administration Guide, McGraw-Hill Companies (2000) available at http://www.books24x7.com/book/id_762/viewer_r.asp?bookid=762&chunkid=410651062 (Goncalves, Check Point FW); Check Point Software Technologies Ltd. (1999) (Check Point FW)	
	D1721	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. CIS/DCOM as described in: Microsoft Corp., Cariplo: Distributed Component Object Model, references (1996-1999)	
	D1722	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Bhattacharya et al., "An LDAP Schema for Configuration and Administration of IPSec Based Virtual Private Networks (VPNs)", IETF Internet Draft (October 1999) ("LDAP Schema for IPSec based VPNs publication")	
	D1723	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Onion Routing references (1996, 1997, 1999	
	D1724	Microsoft Claim Chart of U.S. Patent 6,502,135; vs. Aventail references (1997-1999)	
	D1725	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. C. Huitema et al., "Simple Gateway Control Protocol," Version 1.0 (May 5, 1998) ("SGCP")	
	D1726	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. Microsoft VPN Technology references (1997-1999)	
	D1727	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. Dynamic VPN ("DVPN") references (1997-2001)	
	D1728	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. R.G. Moskowitz, "Network Address Translation Issues with IPsec," Internet Draft, Internet Engineering Task Force, February 6, 1998 ("Moskowitz")	
	D1729	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. F-Secure VPN and F-Secure VPN references (1996, 1998, 1999)	
	D1730	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. Atkinson et al., "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998) ("RFC 2401")	
	D1731	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. RFC 2543 and Internet Drafts (1999)	
	D1732	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. AltaVista Tunnel and/or the AltaVista Firewall references (1997, 1998)	
	D1733	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. Henning Schulzrinne, Personal Mobility for Multimedia Services in the Internet, Proceedings of the European Workshop on Interactive Distributed Multimedia Systems and Services (1996) ("Schulzrinne 96")	
	D1734	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. Schulzrinne U.S. Pat. No. 6,937,597 (August 30, 2005)	
	D1735	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. J.M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California (July 1996) ("Galvin")	
	D1736	Microsoft Claim Chart of U.S. Patent No. 6,502, 135; vs. Naganand Doraswamy, Implementation of Virtual Private Network (VPNs) with IP Secrity [sic] <draft-ietf-ipsec-vpn-00.txt> (March 12, 1997) ("Doraswamy")	
	D1737	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. FreeS/WAN references (1996)	
	D1738	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. 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"); J. Gilmore et al., Re: Key Management, anyone? (DNS keying) IETF IPSec Working Group Mailing List Archive (8/96 - 9/96)	
	D1739	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. the Automotive Network exchange ("ANX) references (1997, 1999)	

/Krisna Lim/

07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1740	Microsoft Claim Chart of U.S. Patent No. 6,502,135; vs. The Defense Information Systems Agency, Secret Internet Protocol router Network (SIPRNET)[1] references (1998, 2000)	
	D1741	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. U.S. Patent Application No. 09/399,753 ("the Miller Application") as published in U.S. Pub. No. 2005/0055306 (Priority Date: 09/22/98)	
	D1742	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. R. Atkinson, "An Internetwork Authentication Architecture," Naval Research Laboratory, Center for High Assurance Computing Systems (8/5/93) ("Atkinson NRL")	
	D1743	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Donald Eastlake, Domain Name System Security Extensions, IETF DNS Security Working Group (December 1998), available at http://www.watersprings.org/pub/id/draft-ietf-dnssec-secext2-07.txt ("DNSSEC-7")	
	D1744	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Goldschlag et al., "Privacy on the Internet," Naval Research Laboratory, Center for High Assurance Computer Systems (1997) ("Goldschlag I")	
	D1745	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Goldschlag et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK (May 1996) ("Goldschlag II")	
	D1746	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Goldschlag et al., "Onion Routing for Anonymous and Private Internet Connection," Naval Research Laboratory, Center for High Assurance Computer Systems (January 28, 1999) ("Goldschlag III)	
	D1747	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. M.G. Reed, et al., "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA Dec. 9-13, 1996 ("Reed")	
	D1748	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. D. MacDonald et al., "PF_KEY Key Management API, Version 2," Network Working Group, RFC 2367 (July 1998) ("RFC 2367")	
	D1749	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Onion Routing, "Investigation of Route Selection Algorithms," available at http://www.onion-router.net/Archives/Route/index.html ("Route Selection")	
	D1750	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Scott et al., Virtual Private Networks, O'Reilly and Associates, Inc., 2nd ed. (Jan. 1999) ("Scott VPNs")	
	D1751	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Syverson et al., "Private Web Browsing," Naval Research Laboratory, Center for High Assurance Computer Systems (June 2, 1997) ("Syverson")	
	D1752	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. SafeNet VPN Products ("SafeNet VPN Products,") (1999-2000)	
	D1753	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. "Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources," FirstVPN, (Jan 2000) ("First VPN Building a Microsoft VPN publication")	
	D1754	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Publicly Available DNS-Related Correspondence dated September 7, 1993 to September 20, 1993 ("DNS-related Correspondence")	
	D1755	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. DNS SRV references (1996, 1998, 1999, 2000)	
	D1756	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. U.S. Pat. No. 5,898,830 ("Wesinger '830 Patent")	
	D1757	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Global VPN references (1999)	
	D1758	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Kaufman et al., Implementing IPsec: Making Security Work on VPNs, Intranets, and Extranets, (Copyright 1999) ("Implementing IPsec")	

/Krisna Lim/

07/01/2014

[1] SIPRNET is a U.S. Government Internet Protocol network for the transport of information classified as SECRET. SIPRNET was built starting in 1995, and contains domain names bearing the ".smil" designation. Microsoft has subpoenaed information from the Department of Defense and others relationg to SIPRNET, and reserves the right to amend its contentions to take any additional information about SIPRNET that it receives into account.Department of Defense and others relationg to SIPRNET, and reserves the right to amend its contentions to take any additional information about SIPRNET that it receives into account.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1759	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. PGP Security, Finding Your Way Through the VPN Maze (1999) ("PGP")	
	D1760	Microsoft Claim Chart of U.S. Patent No. 6,839,759); vs. Safe Surfing: How to Build a Secure World Wide Web Connection, IBM Int'l Technical Support Organization (March 1996) ("Safe Surfing")	
	D1761	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. U.S. Provisional Patent Application No. 60/134,547 (filed May 17,1999) ("Sheymov")	
	D1762	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Data Fellows F-Secure VPN ("F-Secure VPN+ Publication")	
	D1763	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. U.S. Pat. No. 5,950,195 ("Stockwell '195 Patent'")	
	D1764	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. B. Patel et al., "DHCP Configuration of IPSEC Tunnel Mode, "IPSEC Working Group, Internet Draft 02 (10/15/1999) ("Patel")	
	D1765	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. SSL VPNs ("SSL VPNs") references (1996-1997)	
	D1766	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Gauntlet Firewall ("Gauntlet FW") references (19995, 1996, 1999)	
	D1767	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Caronni et al., U.S. Patent No. 5,822,434 October 13, 1998 (filed June 18, 1996) ("434 patent)	
	D1768	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. U.S. Pat. No. 5,311,593 ("'593 patent")	
	D1769	Microsoft Claim Chart of U.S. Patent No. 6,839,759; RFC 2230 (November 1997) U.S. Pat. No. 5,511,122 (April 23, 1996)	
	D1770	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Check Point FW as described in: Goncalves et al., Check Point FireWall-1 Administration Guide, McGraw-Hill Companies (2000) available at http://www.books24x7.com/book/id_762/viewer_r.asp?bookid=762&chunkid=410651062 (Goncalves, Check Point FW); Check Point Software Technologies Ltd. (1999) (Checkpoint FW)	
	D1771	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. CIS/DCOM references (1996, 1997, 1998, 1999)	
	D1772	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Bhattacharya et al., "An LDAP Schema for Configuration and Administration of IPSec Based Virtual Private Networks (VPNs)", IETF Internet Draft (October 1999) ("LDAP Schema for IPSec based VPNs publication")	
	D1773	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Onion Routing references (1996, 1997, 1999)	
	D1774	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Aventail references (1996, 1997, 1999)	
	D1775	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. C. Huitema et al., "Simple Gateway Control Protocol," Version 1.0 (May 5, 1998) ("SGCP")	
	D1776	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Microsoft VPN Technology references (1997-1999)	
	D1777	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Dynamic VPN ("DVPN") references (1997-2001)	
	D1778	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. R.G. Moskowitz, "Network Address Translation Issues with IPsec," Internet Draft, Internet Engineering Task Force, February 6, 1998 ("Moskowitz")	
	D1779	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Ted Harwood, Windows NT Terminal Server and Citrix MetaFrame (New Riders 1999) ("Windows NT Harwood")	
	D1780	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Todd W. Mathers and Shawn P. Genoway, Windows NT Thin Client Solutions: Implementing Terminal Server and Citrix MetaFrame (Macmillan Technical Publishing 1999) ("Windows NT Mathers")	
	D1781	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. F-Secure VPN and F-Secure VPN+ references (1996-1999)	
	D1782	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. TimeStep, "The Business Case for Secure VPNs" (1998) ("TimeStep")	

/Krisna Lim/ 07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1783	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Atkinson et al., "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998) ("RFC 2401")	
	D1784	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. U.S. Pat. No. 6,079,020 ("VPNet '020 Patent")	
	D1785	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. U.S. Pat. No. 6,173,399 ("VPNet '399 Patent")	
	D1786	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. U.S. Pat. No. 6,226,748 ("VPNet '748 Patent")	
	D1787	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. U.S. Pat. No. 6,226,751 ("VPNet '751 Patent")	
	D1788	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Aboba et al., "Securing L2TP using IPSEC," PPPEXT Working Group, Internet Draft (February 2, 1999) ("L2TP/IPSEC")	
	D1789	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. AltaVista Tunnel and/or the AltaVista Firewall references (1997, 1998)	
	D1790	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Henning Schulzrinne, Personal Mobility for Multimedia Services in the Internet, Proceedings of the European Workshop on Interactive Distributed Multimedia Systems and Services (1996) ("Schulzrinne 96")	
	D1791	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. U.S. Pat. No. 6,701,437 ("VPNet '437 Patent")	
	D1792	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. WatchGuard references (2000)	
	D1793	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. J.M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California (July 1996) ("Galvin")	
	D1794	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. Naganand Doraswamy, Implementation of Virtual Private Network (VPNs) with IP Secrity [sic.] <draft-ietf-ipsec-vpn-00.txt> (March 12, 1997) ("Doraswamy")	
	D1795	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. FreeS/WAN references (1996)	
	D1796	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. 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"); J. Gilmore et al., Re: Key Management, anyone? (DNS keying) IETF IPSec Working Group Mailing List Archive (8/96 – 9/96)	
	D1797	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. The Defense Information Systems Agency, Secret Internet Protocol Router Network (SIPRNET) references (1998, 2000)	
	D1798	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Donald Eastlake, Domain Name System Security Extensions, IETF DNS Security Working Group (December 1998), available at http://www.watersprings.org/pub/id/draft-ietf-dnssec-secext2-07/txt ("DNSSEC-7")	
	D1799	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Goldschlag et al., "Privacy on the Internet," Naval Research Laboratory, Center for High Assurance Computer Systems (1997) ("Goldschlag I")	
	D1800	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Goldschlag et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK (May 1996) ("Goldschlag II")	
	D1801	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Goldschlag et al., "Onion Routing for Anonymous and Private Internet Connection," Naval Research Laboratory, Center for High Assurance Computer Systems (January 28, 1999) ("Goldschlag III")	
	D1802	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. M.G. Reed, et al. "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA Dec. 9-13, 1996 ("Reed")	
	D1803	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. D. McDonald et al., "PF_KEY Key Management API, Version 2," Network Working Group, RFC 2367 (July 1998) ("RFC 2367")	
	D1804	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Onion Routing, "Investigation of Route Selection Algorithms," available at http://www.onion-router.net/Archives/Route/index.html ("Route Selection")	

/Krisna Lim/ 07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1805	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Scott et al., Virtual Private Networks, O'Reilly and Associates, Inc., 2nd ed. (Jan. 1999) ("Scott VPNs")	
	D1806	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Syverson et al., "Private Web Browsing," Naval Research Laboratory, Center of High Assurance Computer Systems (June 2, 1997) ("Syverson")	
	D1807	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. "IPSec Minutes from Montreal," IPSEC Working Group Meeting Notes, http://sandleman.ca/ipsec/1996/08/msg00018.html (June 1996)	
	D1808	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. "Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources," FirstVPN, (Jan 2000) ("First VPN Building a Microsoft VPN publication")	
	D1809	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. DNS SRV references (1996, 1998, 1999, 2000)	
	D1810	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. U.S. Pat. No. 5,898,830 ("Wesigner '830 Patent")	
	D1811	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Kaufman et al., Implementing IPsec: Making Security Work on VPNS, Intranets, and Extranets (Copyright 1999) ("Implementing IPsec")	
	D1812	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Safe Surfing: How to Build a Secure World Wide Web Connection, IBM Int'l Technical Support Organization (March 1996) ("Safe Surfing")	
	D1813	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. U.S. Provisional Patent Application No. 60/134,547 (filed May 17, 1999) ("Sheymov")	
	D1814	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Data Fellows F-Secure VPN ("F-Secure VPN+ Publication)	
	D1815	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. U.S. Pat. No. 5,950,195 ("Stockwell '195 Patent")	
	D1816	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. B. Patel et al., "DHCP Configuration of IPSEC Tunnel Mode," IPSEC Working Group, Internet Draft 02 (10/15/1999) ("Patel")	
	D1817	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. SSL VPNs ("SSL VPNs") references (1996, 1999)	
	D1818	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Gauntlet Firewall ("Gauntlet FW") references (1995, 1996, 1999)	
	D1819	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. U.S. Pat. No. 6,199,171 ("'171 patent")	
	D1820	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Caronni et al., U.S. Patent No. 5,822,434 October 13, 1998 (filed June 18, 1996) ("'434 patent")	
	D1821	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. U.S. Pat. No. 6,005,574 ("'574 patent")	
	D1822	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. RFC 2230 (November 1997) ("KX Records"); U.S. Pat. No. 5,511,122 (April 23, 1996)	
	D1823	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Check Point FW as described in: Goncalves et al., Check Point FireWall -1 Administration Guide, McGraw-Hill Companies (2000) available at http://www.books24x7.com/book/id_762/viewer_r.asp?bookid=762&chunkid=410651062 (Goncalves, Check Point FW); Check Point Software Technologies Ltd. (1999) (Checkpoint FW)	
	D1824	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Battacharya et al., "An LDAP Schema for Configuration and Administration of IPSec Based Virtual Private Networks (VPNs)", IETF Internet Draft (October 1999) ("LDAP Schema for IPSec based VPNs publication")	
	D1825	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Onion Routing references (1996, 1997, 1999)	
	D1826	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Aventail references (1997, 1999)	
	D1827	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Microsoft VPN Technology references (1997-1999)	

/Krisna Lim/ 07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1828	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. R.G. Moskowitz, "Network Address Translation Issues with IPsec," Internet Draft, Internet Engineering Task Force, February 6, 1998 ("Moskowitz")	
	D1829	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. RFC 2543 and Internet Drafts (1999)	
	D1830	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. AltaVista Tunnel and/or the AltaVista Firewall references (1997); Birrell et al., U.S. Pat. No. 5,805,803, Sep. 8, 1998 (filed May 13, 1997)	
	D1831	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Henning Schulzrinne, Personal Mobility for Multimedia Services in the Internet, Proceedings of the European Workshop on Interactive Distributed Multimedia Systems and Services (1996) ("Schulzrinne 96")	
	D1832	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. J. M. Gavin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California (July 1996) ("Galvin")	
	D1833	Microsoft Claim Chart of U.S. Patent No. 7,188,180; Naganand Doraswamy, Implementation of Virtual Private Networks (VPNs) with IP Secrity [sic.] <draft-ietf-ipsec-vpn-00.txt> (March 12, 1997) ("Doraswamy")	
	D1834	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. FreeS/WAN references (1996)	
	D1835	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. H. Orman et al., Re: 'Re: DNS? Was Re: Key Management, anyone?, IETF IPSec Working Group Mailing List Archive (9/96 – 9/96) ("Orman DNS"); J. Gilmore et al., Re: Key Management, anyone? (DNS keying) IETF IPSec Working Group Mailing List Archive (8/96 - 9/96)	
	D1836	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. The Defense Information Systems Agency, Secret Internet Protocol Router Network (SIPRNET) references (1998, 2000)	
	D1837	Microsoft Claim Chart of U.S. Patent No. 7,188,180; vs. Dynamic VPN ("DVPN") reference (1997-2001)	
	D1838	Pereira, "Extended Authentication Within ISAKMP/Oakley," IP Security Working Group, Internet Draft (1998)	
	D1839	Patel et al., "Revised SA Negotiation Mode for ISAKMP/Oakley," IP Security Working Group, Internet Draft (1997)	
	D1840	Pereira et al., "The ISAKMP Configuration Method," IP Security Working Group (1998)	
	D1841	Piper, "A GSS-API Authentication Mode for ISAKMP/Oakley," Internet Draft (1997)	
	D1842	Rescorla, "HTTP Over TLS," Internet Draft (1999)	
	D1843	Lottor, "Domain Administrators Operations Guide," RFC 1033 (1987)	
	D1844	Everhart et al., "New DNS RR Definitions," RFC 1183 (1990)	
	D1845	Hardcastle-Kille, "X.500 and Domains, RFC 1279 (1991)	
	D1846	Manning, "DNS NSAP RRS," RFC 1348 (1992)	
	D1847	Huitema, "An Experiment in DNS Based IP Routing," RFC 1383 (1992)	
	D1848	Eastlake, "Physical Link Security Type of Service," RFC 1455 (1993)	
	D1849	Housley, "Security Label Framework for the Internet," RFC ":1457 (1993)	
	D1850	Kastenholz, "The Definitions of Managed Objects for the Security Protocols of the Point to Point Protocol," RFC 1472 (1993)	
	D1851	Kaufman, "DASS Distribution Authentication Security Service," RFC 1507 (1993)	
	D1852	Linn, "Generic Security Service Application Program Interface," RFC 1508 (1993)	
	D1853	Wray, "Generic Security Service API: C-Bindings, RFC 1509 (1993)	

/Krisna Lim/ 07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1854	Postel, "Domain Name System Structure and Delegation," RFC 1591 (1994)	
	D1855	Austein et al., "DNS Server MIB Extension," RFC 1611 (1994)	
	D1856	Austein et al., "DNS Resolver MIB Extensions," RFC 1612 (1994)	
	D1857	Manning et al., "DNS NSAP Resource Records," RFC 1637 (1994)	
	D1858	Allocchio et al., "Using the Internet DNS to Distribute RFC 1327 Mail Address Mapping Tables," RFC 1664 (1994)	
	D1859	Manning et al., "DNS NSAP Resource Records," RFC 1706 (1994)	
	D1860	Farrell et al., "DNS Encoding of Geographical Location," RFC 1712 (1994)	
	D1861	Brisco, "DNS Support for Load Balancing," RFC 1794 (1995)	
	D1862	Atkinson, "IP Authentication Header, RFC 1826 (1995)	
	D1863	Atkinson, "IP Encapsulating Security Payload (ESP)," RFC 1827 (1995)	
	D1864	Metzger, "IP Authentication Using Keyed MDS," RFC 1828 (1995)	
	D1865	Davis et al., "A Means for Expressing Location Information in the Domain Name System," RFC 1876 (1996)	
	D1866	Cobb, "PPP Internet Protocol Extensions for Name Server Addresses," RFC 1877 (1995)	
	D1867	Thomson et al., "DNS Extensions to Support IP Version 6," RFC 1886 (1995)	
	D1868	Linn, "Generic Security Service Application Program Interface, Version 2," RFC 2078 (1997)	
	D1869	Vixie et al., "Dynamic Updates in the Domain Name System (DNS Update)," RFC 2136 (1997)	
	D1870	Eastlake, "Secure Domain Name System Dynamic Update," RFC 2137 (1997)	
	D1871	Rigney et al., "Remote Authentication Dial in User Service (Radius)," RFC 2138 (1997)	
	D1872	Rigney, "RADIUS Accounting," RFC 2139 (1997)	
	D1873	Allocchio, "Using the Internet DNS to Distribute Mixer Conformant Global Address Mapping," RFC 2163 (1998)	
	D1874	Daniel et al., "Resolution of Uniform Identifiers Using the Domain Name System," RFC 2168 (1997)	
	D1875	Elz et al., "Clarifications to the DNS Specification," RFC 2181 (1997)	
	D1876	Hamilton et al., "Use of DNS Aliases for Network Services," RFC 2219 (1997)	
	D1877	Kille et al., "Using Domains in LDAP/X.500 Distinguished Names," RFC 2247 (1998)	
	D1878	Bellovin et al., "Report of the IAB Security Architecture Workshop," RFC 2316 (1998)	
	D1879	Moats et al., "Building Directories from DNS: Experiences from WWWSeeker," RFC 2517 (1999)	
	D1880	Eastlake, "RSA/MD5 Keys and Sigs in the Domain Name System (DNS)," RFC 2537 (1999)	
	D1881	Eastlake, "Storage of Diffle-Hellman Keys in the Domain Name Systems (DNS)," RFC 2539 (1999)	
	D1882	Eastlake, "DNS Security Operational Considerations," RFC 2541 (1999)	
	D1883	Eastlake, "Reserved Top Level DNS Names," RFC 2606 (1999)	
	D1884	Aboba et al., "Proxy Chaining and Policy Implementation in Roaming," RFC 2607 (1999)	

/Krisna Lim/ 07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1885	Vixie, "Extensions Mechanisms for DNS (EDNSO)," RFC 2671 (1999)	
	D1886	Crawford, "Non-Terminal DNS Name Redirection," RFC 2672 (1999)	
	D1887	Srisuresh et al., "Security Model with Tunnel-Mode IPsec for NAT Domains," RFC 2709 (1999)	
	D1888	Eastlake, "Secret Key Establishment for DNS (TKEY RR)," RFC 2930 (2000)	
	D1889	Cisco Security Advisory: PIX Private Link Key Processing and Cryptography Issues (1998) available at http://www.cisco.com/warp/public/707/cisco-sa-19980603-pix-key.shtml	
	D1890	Gauntlet for IRIX Administrator's Guide (1985)	
	D1891	Gauntlet Firewall for UNIX; Administrator's Guide, Version 4.2 (1996-1998)	
	D1892	Gauntlet Firewall for UNIX; Getting Started Guide, Version 4.2 (1996-1998)	
	D1893	Gauntlet Firewall for UNIX; Netperm Table Reference Guide, Version 4.2 (1996-1998)	
	D1894	Gauntlet Firewall for UNIX, User Guide, Version 4.2 (1996-1998)	
	D1895	Snyder "Review: Firewalls," Network World (1998)	
	D1896	Schlaerth, "Service and Network Management Strategies for ATM in Wireless Networks," Bell Labs Technical Journal (2000)	
	D1897	Fischer et al., "Accounting Solutions in the UMTS Core Network," Bell Labs Technical Journal, 6(2):65-73 (2002)	
	D1898	Bakker et al., "Rapid Development and Delivery of Converged Services Using APLS," Bell Labs Technical Journal (2000)	
	D1899	La Roche et al., "High Speed Data Services Using the Switched Digital Broadband Access Systems," Bell Labs Technical Journal (1997)	
	D1900	Mooi Choo Chuah et al., "Mobile Virtual Private Dial-Up Services," Bell Labs Technical Journal (1999)	
	D1901	Fendick et al., "The PacketStar™ 6400 IP Switch – An IP Switch for the Converged Network," Bell Labs Technical Journal (1998)	
	D1902	Schulzrinne et al., "The Session Initiation Protocol: Providing Advanced Telephony Services Across the Internet," Bell Labs Technical Journal (1998)	
	D1903	Moganti et al., "A Framework for Understanding Network Intelligence," Bell Labs Technical Journal (2001)	
	D1904	Bosco et al., "Evolution of the Wide Area Network," Bell Labs Technical Journal (2000)	
	D1905	Raghavan et al., "Virtual Private Networks and Their Role in E-Business," Bell Labs Technical Journal, 6(2):99-115 (2002)	
	D1906	Sijben et al., "Application-Level Control of IP Networks: IP Beyond the Internet," Bell Labs Technical Journal (2001)	
	D1907	Kozik et al., "Voice Services in Next-Generation Networks: The Evolution of the Intelligent Network and its Role in Generating New Revenue Opportunities," Bell Labs Technical Journal (1998)	
	D1908	Brenner et al., "CyberCarrier Service and Network Management," Bell Labs Technical Journal (2000)	
	D1909	Stevens et al., "Policy-Based Management for IP Networks," Bell Labs Technical Journal (1999)	
	D1910	Milonas, "Enterprise Networking for the New Millennium," Bell Labs Technical Journal (2000)	
	D1911	Busschbach, "Toward QoS-Capable Virtual Private Networks," Bell Labs Technical Journal (1998)	
	D1912	McGee et al., "Dynamic Virtual Private Networks," Bell Labs Technical Journal, 6(2):116-135 (2002)	
	D1913	Veeraraghavan, "Connection Control in ATM Networks," Bell Labs Technical Journal (1997)	

/Krisna Lim/ 07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1914	Erfani et al., "Network Management: Emerging Trends and Challenges," Bell Labs Technical Journal (1999)	
	D1915	Rodriguez-Moral, "LIBRA-An Integrated Framework for Type of Service-Based Adaptive Routing in the Internet and Intranets," Bell Labs Technical Journal (1997)	
	D1916	Colbert et al., "Advanced Services: Changing How We Communicate," Bell Labs Technical Journal (2001)	
	D1917	Kocan et al., "Universal Premises Access to Voice Band and ATM Networks Using a Broadband Interworking Gateway," Bell Labs Technical Journal (1998)	
	D1918	Kozik et al., "On Opening PSTN to Enhances Voice/Data Services-The PINT Protocol Solution," Bell Labs Technical Journal (2000)	
	D1919	Doshi et al., "A Comparison of Next-Generation IP-Centric Transport Architectures," Bell Labs Technical Journal (1998)	
	D1920	Bergren et al., "Wireless and Wireline Convergence," Bell Labs Technical Journal (1997)	
	D1921	Al-Salameh et al., "Optical Networking," Bell Lab Technical Journal (1998)	
	D1922	Bauer, "IP Exchange Systems – Redefining Distributed Communications in the Enterprise," Bell Labs Technical Journal," (1999)	
	D1923	Dianda et al., "Reducing Complexity for Converged Voice/Data Networks and Services Architecture," Bell Labs Technical Journal (2000)	
	D1924	Meeuwissen et al., "The FRIENDS Platform-A Software Platform for Advanced Services and Applications," Bell Labs Technical Journal (2000)	
	D1925	Unmehopa et al., "The Support of Mobile Internet Applications in UMTS Networks Through the Open Service Access," Bell Labs Technical Journal 6(2):47-64 (2002)	
	D1926	Varadharajan et al., "Information Security and Privacy; Lecture Notes in Computer Science 1270," (1997)	
	D1927	Cisco Delivers Internet Infrastructure for Carrier-Class Voice Quality, April 28, 1998	
	D1928	Cisco Product Catalog, Cisco IP/VC 3500 Series – Videoconferencing Products, May 2000	
	D1929	Cisco Simplifies H.323 Multimedia Conferencing for Enterprises and Service Providers, April 28, 1998	
	D1930	Kotha, "Deploying H.323 Applications in Cisco Networks," White Paper, Cisco Systems, Inc. (1998)	
	D1931	H.332 Architecture and Design, Cisco Systems (2000)	
	D1932	Empowering The Internet Generation, Cisco Systems, Inc. (2000)	
	D1933	Intel and Cisco Complete Interoperability Tests to Deliver H.323 Connectivity, October 6, 1998	
	D1934	Spectrus Multipoint Video Conferencing Service Operational & Performance Specifications; Technical Reference Guide, Bellsouth, May 1995	
	D1935	Lambert, "IP Service Switches Could Give CLECs Hosted-App Portal Power," July 1, 1999 available at http://www.exhangmag.com/articles/971work1.html	
	D1936	IP Service Intelligence at the Edge; Enabling Value-Added Services Over DSL (April 2000)	
	D1937	Next Generation IP Conferencing Systems, Ridgeway Systems & Software; White Paper (1999)	
	D1938	Gupta et al., "Secure and Mobile Networking," Mobile Networks and Applications, 3:381-390 (1998)	
	D1939	Guin et al., "Application of Virtual Private Networking Technology to Standards-Based Management Protocols Across Heterogeneous Firewall-Protected Networks," IEEE (1999)	
	D1940	Zao et al., "A Public-Key Based Secure Mobile IP," Wireless Networks, J.C. Baltzer AG, Science Publishers, 5:373-390 (1999)	
	D1941	Wirbel, "Upgraded Tools Promse Scalable Virtual Networks," Electronic Engineering Times, pages 60 (1998)	
	D1942	Rescorla et al., "The Secure HyperText Transfer Protocol," RFC 2660 (1999)	

/Krisna Lim/ 07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1943	Lioy et al., "DNS Security," Terena Networking Conference, May 22-25, 2000	
	D1944	Gilmore et al., "Secure Remote Access to an Internal Web Server," IEEE Network (1999)	
	D1945	Kiuchi et al., "Using a WWW-based Mail User Agent for Secure Electronic Mail Service for Health Care Users," Methods of Information in Medicine, 37:247-253 (1998)	
	D1946	Kiuchi et al., "Automated Generation of a World Wide Web-Based Data Entry and Check Program for Medical Applications," Computer Methods and Programs in Biomedicine, 52:129-138 (1996)	
	D1947	Kiuchi et al., "A World Wide Web-Based User Interface for a Data Management System for Use in Multi-Institutional Clinical Trials – Development and Experimental Operation of an Automated Patient Registration and Random Allocation System," Elsevier Science Inc., 17:476-493 (1996)	
	D1948	Kiuchi et al., "University Medical Information Network – Past, Present, and Future," Medinfo (1998)	
	D1949	A Natural Extension of Cisco Systems IP Networking Expertise, The Cisco AS5300/Voice Gateway Relays High Quality Voice and Fax Traffic Across an IP Network, Data Sheet (1999)	
	D1950	Altiga Networks, Building Remote Access VPNs	
	D1951	VPN; The Remote Access Solution, A Comprehensive Guide to Evaluating: Security, Administration, Implementation (1997) available at www.compatible.com	
	D1952	10/100 Ethernet – DES I/O Card Administrator's Guide, Compatible Systems Corporation (1999) available at www.compatible.com	
	D1953	Compatiview 5.4 Reference Guide, Compatible Systems Corporation (1999) www.compatible.com	
	D1954	HSSI-DES I/O Card Administrator's Guide, Compatible Systems Corporation (1999) www.compatible.com	
	D1955	IntraPort 2 and IntraPort 2+ VPN Access Server Installation Guide, Compatible Systems Corporation (1998) www.compatible.com	
	D1956	IntraPortVPN Access Server Installation Guide, Compatible Systems Corporation (1998) www.compatible.com	
	D1957	IntraPort 2 and IntraPort 2+ VPN Access Server Administrator's Guide, Compatible Systems Corporation (1999) www.compatible.com	
	D1958	IntraPort Carrier-2 Chassis Administrator's Guide, Compatible Systems Corporation (1999) www.compatible.com	
	D1959	IntraPort Carrier-8 Chassis Administrator's Guide, Compatible Systems Corporation (1999) www.compatible.com	
	D1960	IntraPort Client Software Reference Guide, Compatible Systems Corporation (1999) www.compatible.com	
	D1961	IntraPort Enterprise-2 VPN Access Server; Administrator's Guide, Compatible Systems Corporation (1999) www.compatible.com	
	D1962	IntraPort Enterprise-8 VPN Access Server; Installation Guide, Compatible Systems Corporation (1999) www.compatible.com	
	D1963	Text-Based Configuration and Command Line Management; Reference Guide, Compatible Systems Corporation (1998) www.compatible.com	
	D1964	VPN Client Software Reference Guide, Compatible Systems Corporation (1999) www.compatible.com	
	D1965	Release Notes for Cisco Secure PIX Firewall Version 5.0(3), Cisco Systems (2000)	
	D1966	Valencia et al., "Cisco Layer Two Forwarding (Protocol) L2F," RFC 2341 (1998)	
	D1967	Schulzrinne, "SIP: Status and Directions," Department of Computer Science, Columbia University (1999)	
	D1968	Schulzrinne, "SIP: More Than Grandma's Phone Calls," Department of Computer Science, Columbia University (1999)	
	D1969	Willis, "The Future is SIP," ISSN: 1046-4468, 10(19):1046-4468 (1999)	

/Krisna Lim/

07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D1970	Borthick, "Convergence Gets Complicated; Industry Trend or Event, ISSN:0162-3885, 29(11):6 (1999)	
	D1971	Vovida Networks and Nuera Communications Team to Enhance Vovida's Free SIP Protocol Stack for Voice over IP Applications; Business Wire (1999)	
	D1972	Kraskey et al., "NPN: Next-Generation Network Voice Services; Internet/Web/Online Service Information," ISSN:1093-8001 (1999)	
	D1973	Lucent Technologies Introduces the Elemedia™ SIP Server, A Software Platform for Integrated IP Telecommunications Services, PR Newswire Association, Inc. PR Newswire (1999)	
	D1974	3Com and Level 3 Test Next Generation of Telephone Systems and IP Networks to Speed the Deployment of New Business and Consumer Services, Business Wire, Inc. (2000)	
	D1975	Stahl, "Domain Administrators Guide," RFC 1032 (1987)	
	D1976	Partridge, "Mail Routing and the Domain System," RFC 974 (1986)	
	D1977	Mockapetris, "Domain System Changes and Observations," RFC 973 (1986)	
	D1978	Harrenstien et al., "DOD Internet Host Table Specification," RFC 952 (1985)	
	D1979	Postel, "Domain Name System Implementation Schedule – Revised," RFC 921 (1984)	
	D1980	Postel, Domain Name System Implementation Schedule – RFC 897 (1984)	
	D1981	Mockapetris, "Domain Name – Concepts and Facilities," RFC 882 (1983)	
	D1982	Postel, "The Domain Name Plan and Schedule," RFC 881 (1983)	
	D1983	Zaw-Sing Su, "The Domain Naming Convention for Internet User Applications," RFC 819 (1982)	
	D1984	Earrenstien et al., "Hostnames Server," RFC 811 (1982)	
	D1985	Postel, "Computer Mail Meeting Notes," RFC 805 (1982)	
	D1986	Luotonen, "Tunneling SSL Through a WWW Proxy," Internet-Draft (1997)	
	D1987	Luotonen, "Tunneling SSL Through a WWW Proxy," Internet-Draft (December 1995)	
	D1988	Luotonen, "Tunneling SSL Through a WWW Proxy," Internet-Draft (November 1995)	
	D1989	Luotonen, "Tunneling SSL Through a WWW Proxy," Internet-Draft (June 1995)	
	D1990	Cooper et al., "The US Domain," RFC 1386 (1992)	
	D1991	Rosenbaum, "Using the Domain Name System to Store Arbitrary String Attributes," Digital Equipment Corp., RFC 1464 (1993)	
	D1992	Cooper et al., "The US Domain," RFC 1480 (1993)	
	D1993	Gavron, "A Security Problem and Proposed Correction with Widely Deployed DNS Software," ACES Research Inc., RFC 1535 (1993)	
	D1994	Kumar et al, "Common DNS Implementation Errors and Suggested Fixes," RFC 1536 (1993)	
	D1995	Beertema, "Common DNS Data File Configuration Errors," RFC 1537 (1993)	
	D1996	Hanks et al., "Generic Routing Encapsulation over IPv4 Networks," RFC 1702 (1994)	
	D1997	Romao, "Tools for DNS Debugging," RFC 1713 (1994)	
	D1998	Eastlake et al., "Randomness Recommendations for Security," RFC 1750 (1994)	
	D1999	Federal Networking Council, "U.S. Government Internet Domain Names," RFC 1811 (1995)	
	D2000	Federal Networking Council, "U.S. Government Internet Domain Names," RFC 1816 (1995)	
	D2001	Karn et al., "The ESP DES-CBC Transform," RFC 1829 (1995)	

/Krisna Lim/ 07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2002	Hinden et al., "IP Version 6 Addressing Architecture," RFC 1884 (1995)	
	D2003	Schulzrinne et al., "RTP: A Transport Protocol for Real-Time Applications," Audio-Video Transport Working Group, RFC 1889 (1996)	
	D2004	Schulzrinne, "RTP Profile for Audio and Video Conferences with Minimal Control," RFC 1890 (1996)	
	D2005	Barr, "Common DNS Operational and Configuration Errors," RFC 1912 (1996)	
	D2006	Rekher et al., "Address Allocation for Private Internets," RFC 1918 (1996)	
	D2007	Deutsch, "ZLIB Compressed Data Format Specification Version 3.3," Network Working Group, RFC 1950 (1996)	
	D2008	Engebretson et al., "Registration in the MIL Domain," RFC 1956 (1996)	
	D2009	Elz et al., "Serial Number Arithmetic," RFC 1982 (1996)	
	D2010	Ohta, "Incremental Zone Transfer in DNS," RFC 1995 (1996)	
	D2011	Vixie, "A Mechanism for Prompt Notification of Zone Changes (DNS Notify)," Network Working Group, RFC 1996 (1996)	
	D2012	Manning et al., "Operational Criteria for Root Name Servers," Network Working Group, RFC 2010 (1996)	
	D2013	Speer et al., "RTP Payload Format of Sun's CellB Video Encoding," Network Working Group, RFC 2029 (1996)	
	D2014	Turletti et al., "RTP Payload Format for H.261 Video Streams," Network Working Group, RFC 2032 (1996)	
	D2015	Der-Danieliantz, "The AM (Armenia) Domain," Network Working Group, RFC 2053 (1996)	
	D2016	Rigney et al., "Remote Authentication Dial in User Service (Radius)," Network Working Group, RFC 2058 (1997)	
	D2017	Oehler et al., "HMAC-MDS IP Authentication with Replay Prevention," Network Working Group, RFC 2085 (1997)	
	D2018	Ashworth, "The Naming of Hosts," Network Working Group, RFC 2100 (1997)	
	D2019	Krawczyk et al., "HMAC: Keyed-Hashing for Message Authentication," Network Working Group, RFC 2104 (1997)	
	D2020	Bradner, "Key Words for Use in RFC s to Indicate Requirement Levels," Network Working Group, RFC 2119 (1997)	
	D2021	Crocker, "Mailbox Names for Common Services, Roles and Functions," Network Working Group, RFC 2142 (1997)	
	D2022	Federal Networking Council, "U.S. Government Internet Domain Names," Network Working Group, RFC 2146 (1997)	
	D2023	Elz et al., "Selection and Operation of Secondary DNS Service," Network Working Group, RFC 2182 (1997)	
	D2024	Zhu, "RTP Payload Format for H.263 Video Streams," Network Working Group, RFC 2190 (1997)	
	D2025	Perkins et al., "RTP Payload for Redundant Audio Data," Network Working Group, RFC 2198 (1997)	
	D2026	Cheng et al., "Test Cases for HMAC-MDS and HMAC-SHA-1," Network Working Group, RFC 2202 (1997)	
	D2027	Vaughan, "A Legal Basis for Domain Name Allocation," Network Working Group, RFC 2240 (1997)	
	D2028	Dierks et al., "The TLS Protocol Version 1.0," Network Working Group, RFC 2246 (1999)	
	D2029	Hoffman et al., "RTP Payload Format for MPEG1/MPEG2 Video," Network Working Group, RFC 2250 (1998)	
	D2030	Howard et al., "An Approach for Using LDAP as a Network Information Service," Network Working Group, RFC 2307 (1998)	

/Krisna Lim/ 07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2031	Andrews, "Negative Caching of DNS Queries (DNS NCACHE)," RFC 2308 (1998)	
	D2032	Eidnes et al., "Classless IN-ADDR.ARPA Delegation," Network Working Group, RFC 2317 (1998)	
	D2033	Schulzrinne et al., "Real Time Streaming Protocol (RTSP)," Network Working Group, RFC 2326 (1998)	
	D2034	Civanlar et al., "RTP Payload Format for Bundled MPEG," Network Working Group, RFC 2343 (1998)	
	D2035	Vaughan, "A Convention for Using Legal Names as Domain Names," Network Working Group, RFC 2352 (1998)	
	D2036	McDonald et al., "PF_Key Key Management API, Version 2," Network Working Group, RFC 2367 (1998)	
	D2037	Hinden et al., "IP Version 6 Addressing Architecture," Network Working Group, RFC 2373 (1998)	
	D2038	Hinden et al., "AN IPv6 Aggregatable Global Unicase Address Format," Network Working Group, RFC 2374 (1998)	
	D2039	Grimstad et al., "Naming Plan for Internet Directory-Enabled Applications," Network Working Group, RFC 2377 (1998)	
	D2040	Pereira, "IP Payload Compression Using DEFLATE," Network Working Group, RFC 2394 (1998)	
	D2041	Friend et al., "IP Payload Compression Using LZS," Network Working Group, RFC 2395 (1998)	
	D2042	Bormann et al., "RTP Payload Format for the 1998 Version of ITU-T Rec. H.263 Video (H.263+)," Network Working Group, RFC 2429 (1998)	
	D2043	Tynan, "RTP Payload Format for BT.656 Video Encoding," Network Working Group, RFC 2431 (1998)	
	D2044	Berc et al., "RTP Payload Format for JPEG-Compressed Video," Network Working Group, RFC 2435 (1998)	
	D2045	Pereira, "The ESP CBC-Mode Cipher Algorithms," Network Working Group, RFC 2451 (1998)	
	D2046	Casner et al., "Compressing IP/UDP/RTP Headers for Low-Speed Serial Links," Network Working Groups, RFC 2508 (1999)	
	D2047	Karn et al., "ICMP Security Failures Messages," Network Working Groups, RFC 2521 (1999)	
	D2048	Karn et al., "Photuris: Session-Key Management Protocol," Network Working Group, RFC 2522 (1999)	
	D2049	Eastlake, "DSA Keys and SIGs in the Domain Name System (DNS)," Network Working Group, RFC 2536 (1999)	
	D2050	Gilligan et al., "Basic Socket Interface Extensions for IPv6," Network Working Group, RFC 2553 (1999)	
	D2051	Newman, "Using TLS with IMAP, POP3 and ACAP," Network Working Group, RFC 2595 (1999)	
	D2052	Franks et al., "HTTP Authentication: Basic and Digest Access Authentication," Network Working Group, RFC 2617 (1999)	
	D2053	Hamzeh et al., "Point-to-Point Tunneling Protocol (PPTP)," Network Working Group, RFC 2637 (1999)	
	D2054	McKay, "RTP Payload Format for PureVoice™ Audio," Network Working Group, RFC 2658 (1999)	
	D2055	Rescorla, "The Secure HyperText Transfer Protocol," Network Working Group, RFC 2660 (1999)	
	D2056	Crawford, "Binary Labels in the Domain Name System," Network Working Group, RFC 2673 (1999)	
	D2057	Fox et al., "Virtual Private Networks Identifier," Network Working Group, RFC 2685 (1999)	
	D2058	Medvinskey, "Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)," Network Working Group, RFC 2712 (1999)	

/Krisna Lim/

07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2059	Rosenberg, et al., "An RTP Payload Format for Generic Forward Error Correction," Network Working Group, RFC 2733 (1999)	
	D2060	Fox et al., "NHRP Support for Virtual Private Networks," Network Working Group, RFC 2735 (1999)	
	D2061	Handley, et al., "Guidelines for Writers of RTP Payload Format Specifications," Network Working Group, RFC 2736 (1999)	
	D2062	Rosenberg et al., "Sampling of the Group Membership in RTP," Network Working Group, RFC 2762 (2000)	
	D2063	Gleeson et al., "A Framework for IP Based Virtual Private Networks," Network Working Group, RFC 2764 (2000)	
	D2064	Hellstrom, "RTP Payload for Text Conversation," Network Working Group, RFC 2793 (2000)	
	D2065	Aboba et al., "Implementation of L2TP Compulsory Tunneling via RADIUS," Network Working Group, RFC 2809 (2000)	
	D2066	Khare et al., "Upgrading to TLS within HTTP/1.1," Network Working Group, RFC 2817 (2000)	
	D2067	Rescorla, "HTTP Over TLS," Network Working Group, RFC 2818 (2000)	
	D2068	Daigle, "A Tangled Web: Issues of I18N, Domain Names, and the Other Internet Protocols," Network Working Group, RFC 2825 (2000)	
	D2069	Internet Architecture Board, "IAB Technical Comment on the Unique DNS Root," Network Working Group, RFC 2826 (2000)	
	D2070	Vixie et al., "Secret Key Transaction Authentication for DNS (TSIG)," Network Working Group, RFC 2845 (2000)	
	D2071	Petrack et al., "The PINT Service Protocol: Extensions to SIP and SDP for IP Access to Telephone Call Services," Network Working Group, RFC 2848 (2000)	
	D2072	Keromytis et al., "The Use of HMAC-RIPEMD-160-96 within ESP and AH," Network Working Group, RFC 2857 (2000)	
	D2073	Civanlar et al., "RTP Payload Format for Real-Time Pointers," Network Working Group, RFC 2862 (2000)	
	D2074	Rigney et al., "Remote Authentication Dial In User Service (RADIUS)," Network Working Group, RFC 2865 (2000)	
	D2075	Crawford et al., "DNS Extensions to Support IPv6 Address Aggregation and Renumbering," Network Working Group, RFC 2874 (2000)	
	D2076	Srisuresh, "Secure Remote Access with L2TP," Network Working Group, RFC 2888 (2000)	
	D2077	Mealling, "The Naming Authority Pointer (NAPTR) DNS Resource Record," Network Working Group, RFC 2915 (2000)	
	D2078	Muthukrishnan et al., "A Core MPLS IP VPN Architecture," Network Working Group, RFC 2917 (2000)	
	D2079	Chen, "Route Refresh Capability for BGP-4," Network Working Group, RFC 2918 (2000)	
	D2080	Eastlake et al., "Domain Name System (DNS) IANA Considerations," Network Working Group, RFC 2929 (2000)	
	D2081	Eastlake et al., DNS Request and Transaction Signatures," Network Working Group, RFC 2931 (2000)	
	D2082	Baugher et al., "Real-Time Transport Protocol Management Information Base," Network Working Group, RFC 2959 (2000)	
	D2083	Donovan, "The SIP INFO Method," Network Working Group, RFC 2976 (2000)	
	D2084	Wellington, "Secure Domain Name System (DNS) Dynamic Update," Network Working Group, RFC 3007 (2000)	
	D2085	Wellington, "Domain Name System Security (DNSSEC) Signing Authority," Network Working Group, RFC 3008 (2000)	
	D2086	Rosenberg et al., "Registration of parityfec MIME Types," Network Working Group, RFC 2000 (2000)	

/Krisna Lim/

07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2087	Kikuchi et al., "RTP Payload Format for MPEG-4 Audio/Visual Streams," Network Working Group, RFC 3016 (2000)	
	D2088	Rosen et al., "Multiprotocol Label Switching Architecture," Network Working Group, RFC 3031 (2001)	
	D2089	Rosen et al., "MPLS Label Stack Encoding," Network Working Group, RFC 3032 (2001)	
	D2090	Anderson et al., "LDP Specification," Network Working Group, RFC 3036 (2001)	
	D2091	Thomas et al., "LDP Applicability," Network Working Group, RFC 3037 (2001)	
	D2092	Luthi, "RTP Payload Format for ITU-T Recommendation G.722.1," Network Working Group, RFC 2001 (2001)	
	D2093	Lennox et al., "Common Gateway Interface for SIP," Network Working Group, RFC 3050 (2001)	
	D2094	Heath et al., "IP Payload Compression Using ITU-T V.44 Packet Method," Network Working Group, RFC 3051 (2001)	
	D2095	Rawat et al., "Layer Two Tunneling Protocol (L2TP) over Frame Relay," Network Working Group, RFC 3070 (2001)	
	D2096	Klensin, "Reflections on the DNS, RFC 1591, and Categories of Domains," Network Working Group, RFC 3070 (2001)	
	D2097	Pall et al., "Microsoft Point-To-Point Encryption (MPPE) Protocol," Network Working Group, RFC 3078 (2001)	
	D2098	Zorn, "Deriving Keys for use with Microsoft Point-to-Point Encryption (MPPE)," Network Working Group, RFC 3079 (2001)	
	D2099	Campbell et al., "Control of Service Context Using SIP Request-URI," Network Working Group, RFC 3087 (2001)	
	D2100	Lewis, "DNS Security Extension Clarification on Zone Status," Network Working Group, RFC 3090 (2001)	
	D2101	Bremen et al., "Robust Header Compression (ROHC): Framework and Four Profiles: RTP, UDP,ESP, and Uncompressed," Network Working Group, RFC 3095 (2001)	
	D2102	Borella et al., "Realm Specific IP: Framework," Network Working Group, RFC 3102 (2001)	
	D2103	Borella et al., "Realm Specific IP: Protocol Specification," Network Working Group, RFC 3103 (2001)	
	D2104	Montenegro et al., "RSIP Support for End-to-End IPsec," Network Working Group, RFC 3104 (2001)	
	D2105	Eastlake, "RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)," Network Working Group, RFC 3110 (2001)	
	D2106	Finlayson, "A More Loss-Tolerant RTP Payload Format for MP3 Audio," Network Working Group, RFC 3119 (2001)	
	D2107	Thomas, "Requirements for Kerberized Internet Negotiation of Keys," Network Working Group, RFC 3129 (2001)	
	D2108	Lewis, "Notes from the State-of-the-Technology: DNSSEC," Network Working Group, RFC 3130 (2001)	
	D2109	Kempf, "Dormant Mode Host Alerting ("IP Paging") Problem Statement," Network Working Group, RFC 3132 (2001)	
	D2110	Verma et al., "L2TP Disconnect Cause Information," Network Working Group, RFC 3145 (2001)	
	D2111	Bush, "Delegation of IP6.ARPA," Network Working Group, RFC 3152 (2001)	
	D2112	Perkins et al., "RTP Testing Strategies," Network Working Group, RFC 3158 (2001)	
	D2113	Huston, "Management Guidelines & Operational Requirements for the Address and Routing Parameter Area Domain ("arpa")," Network Working Group, RFC 3172 (2001)	
	D2114	Shacham et al., "IP Payload Compression Protocol (IPComp)," Network Working Group, RFC 3173 (2001)	

/Krisna Lim/

07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2115	Kobayashi et al., "RTP Payload Format for DV (IEC 61834) Video," Network Working Group, RFC 3189 (2002)	
	D2116	Kobayashi et al., "RTP Payload Format for 12-bit DAT Audio and 20- and 24-bit Linear Sampled Audio," Network Working Group, RFC 3190 (2002)	
	D2117	Patel et al., "Securing L2TP Using IPsec," Network Working Group, RFC 3193 (2001)	
	D2118	Austein, "Applicability Statement for DNS MIB Extensions," Network Working Group, RFC 3197 (2001)	
	D2119	Hoffman, "SMTP Service Extensions for Secure SMTP over Transport Layer Security," Network Working Group, RFC 3207 (2002)	
	D2120	Conrad, "Indicating Resolver Support of DNSSEC," Network Working Group, RFC 3225 (2001)	
	D2121	Gudmundsson, "DNSSEC and IPv6 A6 Aware Server/Resolver Message Size Requirements," Network Working Group, RFC 3226 (2001)	
	D2122	Hardie, "Distributing Authoritative Name Servers via Shared Unicast Addresses," Network Working Group, RFC 3258 (2002)	
	D2123	Rosenberg et al., "SIP: Session Initiation Protocol," Network Working Group, RFC 3261 (2002)	
	D2124	Rosenberg et al., "Reliability of Provisional Responses in the Session Initiation Protocol (SIP)," Network Working Group, RFC 3262 (2002)	
	D2125	Resenberg et al., "Session Initiation Protocol (SIP): Locating SIP Servers," Network Working Group, RFC 3263 (2002)	
	D2126	Rosenberg et al., "An Offer/Answer Model with the Session Description Protocol (SDP)," Network Working Group, RFC 3264 (2002)	
	D2127	Roach et al., "Session Initiation Protocol (SIP)-Specific Event Notification," Network Working Group, RFC 3265 (2002)	
	D2128	Olson et al., "Support for IPv6 in Session Description Protocol (SDP)," Network Working Group, RFC 3266 (2002)	
	D2129	Sjoberg et al., "Real-Time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs," Network Working Group, RFC 3267 (2002)	
	D2130	Chown, "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)," Network Working Group, RFC 3268 (2002)	
	D2131	T'Jones et al., "Layer Two Tunneling Protocol (L2TP0:ATM Access Network Extensions," Network Working Group, RFC 3301 (2002)	
	D2132	Srisuresh et al., "Middlebox Communication Architecture and Framework," Network Working Group, RFC 3303 (2002)	
	D2133	Calhoun et al., "Layer Two Tunneling Protocol (L2TP) Differentiated Services Extension," Network Working Group, RFC 3308 (2002)	
	D2134	Niemi et al., "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)," Network Working Group, RFC 3310 (2002)	
	D2135	Rosenberg, "The Session Initiation Protocol (SIP) Update Method," Network Working Group, RFC 3311 (2002)	
	D2136	Camarillo et al., "Integration of Resource Management and SIP," Network Working Group, RFC 3312 (2002)	
	D2137	Marshall, "Private Session Initiation," Private Session Initiation Protocol (SIP) Extensions for Media Authorization," Network Working Group, RFC 3313 (2003)	
	D2138	Wasserman, "Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards," Network Working Group, RFC 3314 (2002)	
	D2139	Schulzrinne et al., "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers," Network Working Group, RFC 3319 (2003)	
	D2140	Price et al., "Signaling Compression (SigComp)," Network Working Group, RFC 3320 (2003)	
	D2141	Hannu et al., "Signaling Compression (SigComp) – Extended Operations," Network Working Group, RFC 3321 (2003)	

/Krisna Lim/

07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2142	Hannu et al., "Signaling Compression (SigComp) Requirements & Assumptions," Network Working Group, RFC 3322 (2003)	
	D2143	Peterson, "A Privacy Mechanism for the Session Initiation Protocol," Network Working Group, RFC 3323 (2002)	
	D2144	Watson, "Short Term Requirements for Network Asserted Identity," Network Working Group, RFC 3324 (2002)	
	D2145	Jennings et al., "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks," Network Working Group, RFC 3325 (2002)	
	D2146	Schulzrinne et al., "The Reason Header Field for the Session Initiation Protocol (SIP)," Network Working Group, RFC 3326 (2002)	
	D2147	Willis et al., "Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contracts," Network Working Group, RFC 3327 (2002)	
	D2148	Arkko et al., "Security Mechanism Agreement for the Session Initiation Protocol (SIP)," Network Working Group, RFC 3329 (2003)	
	D2149	Charlton et al., "User Requirements for the Session Initiation Protocol (SIP) in Support of Deaf, Hard of Hearing and Speech-Impaired Individuals," Network Working Group, RFC 3351 (2002)	
	D2150	Singh et al., "Layer Two Tunneling Protocol (L2TP) Over ATM Adaptation Layer 5 (AAL5)," Network Working Group, RFC 3355 (2002)	
	D2151	Schulzrinne, "Dynamic Host Configuration Protocol (DHCP-for-Ipv4) Option for Session Initiation Protocol (SIP) Servers," Network Working Group, RFC 3361 (2002)	
	D2152	Bush et al., "Representing Internet Protocol Version 6 (IPv6) Addresses in the Domain Name System (DNS)," Network Working Group, RFC 3363 (2002)	
	D2153	Austein, "Tradeoffs in Domain Name System (DNS) Support for Internet Protocol Version 6 (IPv6)," Network Working Group, RFC 3364 (2002)	
	D2154	Caves et al., "Layer Two Tunneling Protocol "L2TP" Management Information Base," Network Working Group, RFC 3371 (2002)	
	D2155	Vemuri et al., "Session Initiation Protocol for Telephone (SIP-T): Context and Architectures," Network Working Group, RFC 3372 (2002)	
	D2156	Camarillo et al., "Grouping of Media Lines in the Session Description Protocol (SDP)," Network Working Group, RFC 338 (2002)	
	D2157	Zopf, "Real-Time Transport Protocol (RTP) Payload for Comfort Noise (CN)," Network Working Group, RFC 3389 (2002)	
	D2158	Camarillo et al., "Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping," Network Working Group, RFC 3398 (2002)	
	D2159	Mealling, "Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS," Network Working Group, RFC 3401 (2002)	
	D2160	Mealling, "Dynamic Delegation Discovery System (DDDS) Part Two: The Algorithm," Network Working Group, RFC 3402 (2002)	
	D2161	Mealling, "Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database," Network Working Group, RFC 3403 (2002)	
	D2162	Mealling, "Dynamic Delegation Discovery System (DDDS) Part Four: The Uniform Resource Identifiers (URI) Resolution Application," Network Working Group, RFC 3404 (2002)	
	D2163	Mealing, "Dynamic Delegation Discovery System (DDDS) Part Five: URI.ARPA Assignment Procedures," Network Working Group, RFC 3405 (2002)	
	D2164	Andersen, "Session Description Protocol (SDP) Simple Capability Declaration," Network Working Group, RFC 3407 (2002)	
	D2165	Sparks, "Internet Media Type Message/Sipfrag," Network Working Group, RFC 3420 (2002)	
	D2166	Lawrence, "Obsoleting Iquery," Network Working Group, RFC 3425 (2002)	
	D2167	Mankin et al., "Change Process for the Session Initiation Protocol (SIP)," Network Working Group, RFC 3427 (2002)	
	D2168	Campbell et al., "Session Initiation Protocol (SIP) Extension for Instant Messaging," Network Working Group, RFC 3428 (2002)	

/Krisna Lim/

07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2169	Palter et al., "Layer-Two Tunneling Protocol Extension for PPP Link Control Protocol Negotiation," Network Working Group, RFC 3437 (2002)	
	D2170	Massay et al., "Limiting the Scope of the KEY Resource Record," Network Working Group, RFC 3445 (2002)	
	D2171	Garcia-Martin, "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)," Network Working Group, RFC 3455 (2003)	
	D2172	Patel et al., "Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPsec Tunnel Mode," Network Working Group, RFC 3456 (2003)	
	D2173	Kelly et al., "Requirements for IPsec Remote Access Scenarios," Network Working Group, RFC 3457 (2003)	
	D2174	Klensin, "Role of the Domain Name System (DNS)," Network Working Group, RFC 3467 (2003)	
	D2175	Garcia-Martin, "The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Static Dictionary for Signaling Compression (SigComp)," Network Working Group, RFC 3485 (2003)	
	D2176	Camarillo, "Compressing the Session Initiation Protocol (SIP)," Network Working Group, RFC 3486 (2003)	
	D2177	Schulzrinne, "Requirements for Resource Priority Mechanisms for the Session Initiation Protocol (SIP)," Network Working Group, RFC 3487 (2003)	
	D2178	Faltstrom et al., "Internationalizing Domain Names in Applications (IDNA)," Network Working Group, RFC 3490 (2003)	
	D2179	Hoffman et al., "Nameprep: A Stringprep Profile for Internationalized Domain Names (IDN)," Network Working Group, RFC 3491 (2003)	
	D2180	Costello, "Punycode: A Bootstring Encoding of Unicode for Internationalized Domain Names in Applications (IDNA)," Network Working Group, RFC 3492 (2003)	
	D2181	Gilligan et al., "Basic Socket interface Extensions for IPv6," Network Working Group, RFC 3493 (2003)	
	D2182	Gharai et al., "RTP Payload Format for Society of Motion Picture and Television Engineers (SMPTE) 292M Video," Network Working Group, RFC 3497 (2003)	
	D2183	Hinden et al., "Internet Protocol Version 6 (IPv6) Addressing Architecture," Network Working Group, RFC 3513 (2003)	
	D2184	Sparks, "The Session Initiation Protocol (SIP) Refer Method," Network Working Group, RFC 3515 (2003)	
	D2185	Camarillo et al., "Mapping of Media Streams to Resource Reservation Flows," Network Working Group, RFC 3524 (2003)	
	D2186	Kivinen et al., "More Modular Exponential (MODP) Diffie-Hellman Groups for Internet Key Exchange (IKE)," Network Working Group, RFC 3526 (2003)	
	D2187	Koren et al., "Enhanced Compressed RTP (CRTP) for Links with High Delay, Packet Loss and Reordering," Network Working Group, RFC 3545 (2003)	
	D2188	Blake-Wilson et al., "Transport Layer Security (TLS) Extensions," Network Working Group, RFC 3546 (2003)	
	D2189	Baugher et al., "The Group Domain of Interpretation," Network Working Group, RFC 3547 (2003)	
	D2190	Schulzrinne et al., "RTP: A Transport Protocol for Real-Time Applications," Network Working Group, RFC 3550 (2003)	
	D2191	Schulzrinne et al., "RTP Prole for Audio and Video Conferences with Minimal Control," Network Working Group, RFC 3551 (2003)	
	D2192	Bellovin et al., "On the Use of Stream Control Transmission Protocol (SCTP) with IPsec," Network Working Group, RFC 3554 (2003)	
	D2193	Casner et al., "MIME Type Registration of RTP Payload Formats," Network Working Group, RFC 3555 (2003)	
	D2194	Xie, "RTP Payload Format for European Telecommunications Standards Institute (ETSI) European Standard ES 201 108 Distributed Speech Recognition Encoding," Network Working Group, RFC 3557 (2003)	

/Krisna Lim/

07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2195	Li, "RTP Payload Format for Enhanced Variable Rate Codecs (EVRC) and Selectable Mode Vocoders (SMV)," Network Working Group, RFC 3558 (2003)	
	D2196	Press Release, Microsoft releases Windows NetMeeting 3 to the Web; New Version Now Available for Download (1999)	
	D2197	Microsoft Windows NetMeeting 3 Readme Windows 2000, Microsoft Corporation Business Review (1999)	
	D2198	Microsoft Windows NetMeeting 3.03 Beta 1 Readme, Microsoft Corporation (1999)	
	D2199	Baan Midmarket Solutions (BMS), Baan Can Company ,Microsoft Corporation Business Review (1998)	
	D2200	Portland Trail Blazers, Business Review, Microsoft Corporation Business Review (1998)	
	D2201	Deere & Company, Intranet Solutions, Microsoft Corporation Business Review (1997)	
	D2202	Dow Chemical, Microsoft Corporation Business Review (1998)	
	D2203	FileNet Corporation, Netmeeting, Microsoft Corporation Business Review (1997)	
	D2204	Ford Motor Company, Netmeeting, Microsoft Corporation Business Review (1997)	
	D2205	Irving, "Meet Me on the Internet," Internet Magazine Archive, Microsoft Corporation (1997)	
	D2206	Microsoft Netmeeting and the Role of Internet Conferencing for Deaf and Hard-of-Hearing Users, Netmeeting, Microsoft Corporation (1997)	
	D2207	Northrop Grumman, Microsoft Corporation Business Review (1998)	
	D2208	The Tompkins Group, Netmeeting, Microsoft Corporation Business Review (1997)	
	D2209	Toys "R" Us, Microsoft Business Review (1998)	
	D2210	Windows NetMeeting, Overview an Direction, Microsoft Corporation (1999)	
	D2211	PC Expo in New York, Technology for Business, Miller Freeman Group (1997-1999)	
	D2212	Microsoft Windows NetMeeting 3 Resource Kit, The Technical Guide to Installing, Configuring, and Supporting NetMeeting 3 in your Organization, Microsoft Corporation (1996-1999)	
	D2213	Hayes et al., Microsoft NetMeeting 3.0 Security Assessment and Configuration Guide, Systems and Network Attack Center, Version 1.14 (2001)	
	D2214	Schulzrinne, "The Session Initiation Protocol (SIP), Columbia University (1998-1999)	
	D2215	NetMeeting Data Conferencing Strategy, Microsoft Corporation (1998)	
	D2216	Integrating NetMeeting & TAPI 3.0, NetMeeting Development Team TAPI 3.0 IP Telephony Team, Microsoft Corporation (October 28, 1998)	
	D2217	Microsoft Windows NetMeeting 3 Resource Kit, The Technical Guide to Installing, Configuring, and Supporting NetMeeting 3 in your Organization, Microsoft Corporation (1996-2001)	
	D2218	ITU-T Recommendation T.127 "Terminals for Telematic Services –Multipoint Binary File Transfer Protocol," Telecommunication Standardization Sector of ITU (1995)	
	D2219	ITU-T Recommendation T.128 "Terminals for Telematic Services –Multipoint Application Sharing," Telecommunication Standardization Sector of ITU (1998)	
	D2220	ITU-T Recommendation T.140 "Series T: Terminal Equipment and Protocols for Telematic Services; Text Conversation Protocol for Multimedia Application," ITU-T – Telecommunication Standardization Sector of ITU (1997)	
	D2221	Buddy List: A Whitepaper, Microsoft Corporation (1997)	
	D2222	Corporate Remote Access Alternatives – iPass White Paper, November 21, 1998, iPass, Inc. ("IPASS")"	
,	D2223	International Technical Support Organization, "Understanding OSF DCE 1.1 for AIX and OS/2," IBM (1995)	

/Krisna Lim/

07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2224	Wenger et al., "RTP Payload Format for H.264 Video," Network Working Group, RFC 3984 (2005)	
	D2225	Bryant et al., "Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture," Network Working Group, RFC 3985 (2005)	
	D2226	Berners-Lee, et al., "Uniform Resource Identifier (URI): Generic Syntax," Network Working Group, RFC 3986 (2005)	
	D2227	Duerst, et al., "International Resource Identifiers (IRIs)," Network Working Group, RFC 3987 (2005)	
	D2228	Schulzrinne, "Indication of Message Composition for Instant Messaging," Network Working Group, RFC 3994 (2005)	
	D2229	SonicWall/Aventail Whitepaper, SSL VPN Combined with Network Security. SonicWALL Clean VPN (2008)	
	D2230	Anyware Technology Announces Java Technology Security Product for Internet Communications, EverLink Suite Provides Secure Remote Network Access Via the Internet, (1998)	
	D2231	RSA Provides Security for Anyware Technology's Java-Based Internet Communications Product, EverLink Suite Incorporates RSA Technology to Provide Secure Remote Network Access, (1998)	
	D2232	Anyware Technology to Introduce New Channel Partner Program During Varvision 1998, Media Alert (1998)	
	D2233	Anyware Technology Launches Channel Partner Program, Company Builds VAR Channel for Its Everlink Suite of Secure Remote Access and Communications Software, News for Immediate Release (1998)	
	D2234	Anyware Technology Adds Three New Key Personnel, Fast Growing Software Developer Hires Director of Channel Sales, Telemarking Account Manager and Quality Assurance Engineer, News for Immediate Release (1998)	
	D2235	Anyware Technology Ships EverLink, The World's First Personal Virtual Private Network Software, News for Immediate Release (1998)	
	D2236	Anyware Technology Includes 30-Day Trial of Esafe Anti-Virus/Anti Vandal Software With Its Personal VPN Product, Pioneer of Remote Access & Secure Communications Software Partners with ESafe Technologies to Enhance EverLink Suite with Anti-Virus/Anti-Vandal Protection, News for Immediate Release (1998)	
	D2237	Anyware Technology Announces Strategic Var Partnerships with Codaram Corporation and RF Microsystems, Resellers Bring EverLink Suite of Secure Remote Access and Communications Software to Two Specific Vertical and Regional Markets, News for Immediate Release (1998)	
	D2238	Anyware Technology Ships New Version of Everlink Suite, Software Upgrade Brings New Levels of Flexibility and Ease of Use to Instant Secure Remote Access and Communications, News for Immediate Release (1999)	
	D2239	Quittek et al., "Definitions of Managed Objects for Robust Header Compression (ROHC)," Network Working Group, RFC 3816 (2004)	
	D2240	Townsley et al., "Layer 2 Tunneling Protocol (L2TP) Active Discovery Relay for PPP over Ethernet (PPPoE)," Network Working Group, RFC 3817 (2004)	
	D2241	Peterson et al., "Using E.164 Numbers with the Session Initiation Protocol (SIP)," Network Working Group, RFC 3824 (2004)	
	D2242	Polk et al., "Dynamic Host Configuration Protocol Option for Coordinate-Based Location Configuration Information," Network Working Group, RFC 3825 (2004)	
	D2243	Arkko et al., "MIKEY: Multimedia Internet KEYing," Network Working Group, RFC 3830 (2004)	
	D2244	Atkins et al., "Threat Analysis of the Domain Name System (DNS)," Network Working Group, RFC 3833 (2004)	
	D2245	Rosenberg et al., "Indicating User Agent Capabilities in the Session Initiation," Network Working Group, RFC 3840 (2004)	
	D2246	Rosenberg et al., "Caller Preferences for the Session Initiation Protocol (SIP)," Network Working Group, RFC 3841 (2004)	

/Krisna Lim/ 07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2247	Mahy, "A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)," Network Working Group, RFC 3842 (2004)	
	D2248	Schlyter, "DNS Security (DNSSEC) NextSECure (NSEC) RDATA Format," Network Working Group, RFC 3845 (2004)	
	D2249	Peterson, "S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)," Network Working Group, RFC 3853 (2004)	
	D2250	Rosenberg, "A Presence Event Package for the Session Initiation Protocol (SIP)," Network Working Group, RFC 3856 (2004)	
	D2251	Rosenberg, "A Watcher Information Event Template-Package for the Session Initiation Protocol (SIP), Network Working Group, RFC 3857 (2004)	
	D2252	Rosenberg, "An Extensible Markup Language (XML) Based Format for Watcher Information," Network Working Group, RFC 3858 (2004)	
	D2253	Peterson, "Common Profile for Presence (CPP)," Network Working Group, RFC 3859 (2004)	
	D2254	Peterson, "Common Profile for Instance Messaging (CPIM)," Network Working Group, RFC 3860 (2004)	
	D2255	Peterson, "Address Resolution for Instant Messaging and Presence," Network Working Group, RFC 3861 (2004)	
	D2256	Klyne et al, "Common Presence and Instant Messaging (CPIM): Message Format," Network Working Group, RFC 3862 (2004)	
	D2257	Sugano et al., "Presence Information Data Format (PIDF)," Network Working Group, RFC 3863 (2004)	
	D2258	Lennox et al., "Call Processing Language (CPL): A Language for User Control of Internet Telephony Services," Network Working Group, RFC 3880 (2004)	
	D2259	Touch et al., "Use of IPsec Transport Mode for Dynamic Routing," Network Working Group, RFC 3884 (2004)	
	D2260	Westerlund, "A Transport Independent Bandwidth Modifier for the Session Description Protocol (SDP)," Network Working Group, RFC 3890 (2004)	
	D2261	Mahy et al., "The Session Initiation Protocol (SIP) "Replaces" Header," Network Working Group, RFC 3891 (2004)	
	D2262	Sparks, "The Session Initiation Protocol (SIP) Referred-Vs. Mechanism," Network Working Group, RFC 3892 (2004)	
	D2263	Peterson, "Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) Format," Network Working Group, RFC 3892 (2004)	
	D2264	Durand et al., "DNS IPv6 Transport Operational Guidelines," Network Working Group, RFC 3901 (2004)	
	D2265	Niemi, "Session Initiation Protocol (SIP) Extension for Event State Publication," Network Working Group, RFC 3903 (2004)	
	D2266	Gurbani et al., "The Spirits (Services in PSTN Requesting Internet Services) Protocol," Network Working Group, RFC 3910 (2004)	
	D2267	Mahy et al., "The Session Initiation Protocol (SIP) "Join" Header," Network Working Group, RFC 3911 (2004)	
	D2268	Xiao et al., "Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)," Network Working Group, RFC 3916 (2004)	
	D2269	Lau et al., "Layer Two Tunneling Protocol – Version 3 (L2TPv3)," Network Working Group, RFC 3931 (2005)	
	D2270	Friend, "Transport Layer Security (TLS) Protocol Compression Using Lempel-Ziv-Stac (LZS)," Network Working Group, RFC 3943 (2004)	
	D2271	Kivinen et al., "Negotiation of NAT-Traversal in the IKE," Network Working Group, RFC 3947 (2005)	
	D2272	Huttunen et al., "UDP Encapsulation of IPsec ESP Packets," Network Working Group, RFC 3948 (2005)	
	D2273	Duric, "Real-Time Transport Protocol (RTP) Payload Format for Internet Low Bit Rate Codec (iLBC) Speech," Network Working Group, RFC 3952 (2004)	

/Krisna Lim/ 07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2274	Peterson, "Telephone Number Mapping (ENUM) Service Registration for Presence Services," Network Working Group, RFC 3953 (2005)	
	D2275	Daigle et al., "Domain-Based Applications Service Location Using SRV RRS and the Dynamic Delegation Discovery Service (DDDS)," Network Working Group, RFC 3958 (2005)	
	D2276	Camarillo, "The Early Session Disposition Type for the Session Initiation Protocol (SIP)," Network Working Group, RFC 3959 (2004)	
	D2277	Camarillo et al, "Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP), Network Working Group, RFC 3960 (2004)	
	D2278	Schulzrinne, "The tel URI for Telephone Numbers," Network Working Group, RFC 3966 (2004)	
	D2279	Camarillo, "The Internet Assigned Number Authority (IANA) Header Field Parameter Registry for the Session Initiation Protocol (SIP)," Network Working Group, RFC 3968 (2004)	
	D2280	Camarillo, "The Internet Assigned Number Authority (IANA) Uniform Resource Identifier (URI) Parameter Registry for the Session Initiation Protocol (SIP)," Network Working Group, RFC 3969 (2004)	
	D2281	Gurbani et al., "Interworking SIP and Intelligent Network (IN) Applications," Network Working Group, RFC 3976 (2005)	
	D2282	Frankel, et al, "The AES-XCBC-MAC-96 Algorithm and Its use with IPsec," Network Working Group, RFC 3556 (2003)	
	D2283	Goyret, "Signaling of Modem-On-Hold Status in Layer 2 Tunneling Protocol (L2TP)," Network Working Group, RFC 3573 (2003)	
	D2284	Soininen, "Transition Scenarios for 3GPP Networks," Network Working Group, RFC 3574 (2003)	
	D2285	Camarillo et al., "Mapping of Integrated Services Digital Network (ISDN) User Part (ISUP) Overlap Signaling to the Session Initiation Protocol (SIP)," Network Working Group, RFC 3578 (2003)	
	D2286	Rosenberg et al., "An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing," Network Working Group, RFC 3581 (2003)	
	D2287	Jason et al., "IPsec Configuration Policy Information Model," Network Working Group, RFC 3585 (2003)	
	D2288	Blaze et al., "IP Security Policy (IPSP) Requirements," Network Working Group, RFC 3586 (2003)	
	D2289	Thompson et al., "DNS Extensions to Support IP Version 6," Network Working Group, RFC 3596 (2003)	
	D2290	Gustafsson, "Handling of Unknown DNS Resource Record (RR) Types," Network Working Group, RFC 3597 (2003)	
	D2291	Frankel et al., "The AFS-CBC Cipher Algorithm and its use with IPsec," Network Working Group, RFC 3602 (2003)	
	D2292	Marshall et al., "Private Session Initiation Protocol (SIP) Proxy-to-Proxy Extensions for Supporting the PacketCable Distributed Call Signaling Architecture," Network Working Group, RFC 3603 (2003)	
	D2293	Huitema, "Real Time Control Protocol (RTCP) Attribute in Session Description Protocol," Network Working Group, RFC 3605 (2003)	
	D2294	Willis et al., "Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration," Network Working Group, RFC 3608 (2003)	
	D2295	Friedman et al., "RTP Control Protocol Extended Reports (RTCP XR)," Network Working Group, RFC 3611 (2003)	
	D2296	Van Der Meer et al., "RTP Payload Format for Transport of MPEG-4 Elementary Streams," Network Working Group, RFC 3640 (2003)	
	D2297	Kwan et al., "Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG)," Network Working Group, RFC 3645 (2003)	
	D2298	Droms, "DNS Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," Network Working Group, RFC 3646 (2003)	

/Krisna Lim/

07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2299	Wellington et al., "Redefinition of DNS Authenticated Data (AD) Bit," Network Working Group, RFC 3655 (2003)	
	D2300	Gudmudsson, "Delegation Signer (DS) Resource Record (RR)," Network Working Group, RFC 3658 (2003)	
	D2301	Johnston et al., "Session Initiation Protocol (SIP) Basic Call Flow Examples," Network Working Group, RFC 3665 (2003)	
	D2302	Johnston et al., "Session Initiation Protocol (SIP) Public Switched Telephone Network (PSTN) Call Flows," Network Working Group, RFC 3666 (2003)	
	D2303	Rosenberg, "A Session Initiation Protocol (SIP) Event Package for Registrations," Network Working Group, RFC 3680 (2004)	
	D2304	Housley, "Using Advanced Encryption Standard (AES) Counter Mode with IPsec Encapsulating Security Payload (ESP)," Network Working Group, RFC 3686 (2004)	
	D2305	Cuellar et al., "Geopriv Requirements," Network Working Group, RFC 3693 (2004)	
	D2306	Danley et al., "Threat Analysis of the Geopriv Protocol," Network Working Group, RFC 3694 (2004)	
	D2307	Klensin, "Application Techniques for Checking and Transformation of Names," Network Working Group, RFC 3696 (2004)	
	D2308	Loughney et al., "Authentication, Authorization and Accounting Requirements for the Session Initiation Protocol (SIP)," Network Working Group, RFC 3702 (2004)	
	D2309	Huang et al., "A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers," Network Working Group, RFC 3706 (2004)	
	D2310	Baugher et al., "The Secure Real-Time Transport Protocol (SRTP)," Network Working Group, RFC 3711 (2004)	
	D2311	Aboba et al., "IPsec-Network Address Translation (NAT) Compatibility Requirements," Network Working Group, RFC 3715 (2004)	
	D2312	Aboba et al., "Securing Block Storage Protocols Over IP," Network Working Group, RFC 3723 (2004)	
	D2313	Rosenberg et al., "Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)," Network Working Group, RFC 3725 (2004)	
	D2314	Hollenbeck, "Transport Layer Security Protocol Compression Methods," Network Working Group, RFC 3749 (2004)	
	D2315	Nikander et al, "IPv6 Neighbor Discovery (ND) Trust Models and Threats," Network Working Group, RFC 3756 (2004)	
	D2316	Kolkman et al., "Domain in Name System Key (DNSKEY) Resource Record (RR) Secure Entry Point (SEP) Flag," Network Working Group, RFC 3757 (2004)	
	D2317	Faltstrom et al., "The E. 164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)," Network Working Group, RFC 3761 (2004)	
	D2318	Peterson, "Enumservice Registration for Session Initiation Protocol (SIP) Addresses of Record," Network Working Group, RFC 3764 (2004)	
	D2319	Arkko et al, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents," Network Working Group, RFC 3776 (2004)	
	D2320	Nagarajan, "Generic Requirements for Provider Provisioned Virtual Private Networks (PPVPN),"3809 (2004)	
	D2321	"Altiga Proves Multi-Vendor Interoperability for Seamless VPN Deployment; VPN Workshop Marks Significant Development in the VPN Market," Business Publications, Business Wire July 12, 1999	
	D2322	Thomas, "Recipe for E-Commerce,", IEEE Internet Computing, (1997) available for download at http://computer.org/internet/	
	D2323	Vyncke, "Build a Site to Site VPN Without Static Address," (1999)	

/Krisna Lim/

07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2324	Altiga Networks, Inc., Altiga VPN Concentrator Series (C50) Versus Nortel Networks Contivity Extranet Switch 4000 and 45000, VPN Tunneling Competitive Evaluation, The Tolly Group, (1999)	
	D2325	International Telecommunication Union; H.323, Series H: Audiovisual and Multimedia Systems; Infrastructure of Audiovisual Services – Systems and Terminal Equipment for Audiovisual Services (1999)	
	D2326	Cisco Systems, VPN 3000 Concentrator Series, User Guide; Release 2.5 (2000)	
	D2327	Cisco Systems, VPN 3000 Concentrator Series, Getting Started; Release 2.5 (2000)	
	D2328	Cisco Systems, VPN 3000 Client, User Guide; Release 2.5 (2000)	
	D2329	Cisco Simplifies H.323 Multimedia Conferencing for Enterprises and Service Providers, Multimedia Conference Manager Provides Policy Management for Voice over IP and Videoconferencing (1998) Article Available at http://web.archive.org/web/200006231265145/www.cisco.com/warp/public/146/pressroom/1998/apr98/25html	
	D2330	IP and Frame Relay: Bridging the Gap for Seamless and Secure Virtual Private Networking, White Paper, Cosine Communications (1998-2000)	
	D2331	Cisco Systems, Cisco IP/VC Quick Product Overview (1999)	
	D2332	Aziz et al., “Simple Key-Management for Internet Protocols,” IPSEC Working Group, Internet Draft (1996)	
	D2333	Karn et al., “Photuris: Session-Key Management Protocol,” Network Working Group, Internet Draft (1997)	
	D2334	Microsoft Claim Chart of U.S. Patent No. 6,839,759; vs. the Automative Network eXchange (“ANX) references (1997, 1999)	
	D2335	Akamatsu et al., “Construction of Infrastructure for Global R&D,” Omron Technics, 38(3) Consecutive No. 127 (1998)	
	D2336	Zimmerer et al., “MIME Media Types for ISUP and QSIG Objects,” Network Working Group, Request for Comments: 3204 (2001)	
	D2337	Karn et al, “Photuris: Extended Schemes and Attributes,” Network Working Group, Request for Comments: 2523 (1999)	
	D2338	Klensin et al., “Domain Names and Company Name Retrieval,” Network Working Group, Request for Comments: 2345 (1998)	
	D2339	Gilligan et al., “Basic Socket Interface Extensions for IPv6,” Network Working Group, Request for Comments: 2133 (1997)	
	D2340	Libes, “Choosing a Name for Your Computer,” Network Working Group, Request for Comments: 1178 (1990)	
	D2341	Young, “New Protocol Connects Voice Over IP,” NetworkWorldFusion, Network World 12/13/1999	
	D2342	Mockapetris, “Domain Names – Implementation and Specification,” Network Working Group, Request for Comments: 883 (1983)	
	D2343	Handley, “Session Invitation Protocol,” Internet Engineering Task Force, Internet Draft (1996)	
	D2344	Berners-Lee, et al., “Uniform Resource Locators (URL),” Network Working Group, Request for Comments: 1738 (1994)	
	D2345	Response to RFP: Altiga, Network World Fusion, May 10, 1999	
	D2346	Agreement dated June 8, 1999 between Microsoft and Limelight Regarding Event Rental Charge.	
	D2347	Microsoft Netmeeting Conferencing Software, San Diego State University, Case Study Library (1999)	
	D2348	Networked Multimedia Technologies Enable Stanford Collaborative Learning Program, Stanford University: Creating a Virtual Master Builder Atelier, Draft: September 28, 1998	
	D2349	Compatible Systems Corporation; CompatiView 4 Reference Guide 1995-1997	

07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT VS. APPLICANT** *(Use as many sheets as necessary)*	**Complete if Known**	
	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2350	Remote Access VPN User Authentication Model – VPN/VLAN Textbook, September 11, 1999." (English Abstract not Available)	
	D2351	Cisco PIX Firewall Series 1992-1999	
	D2352	IPR2014-00481; Inter Partes Review of Patent Number 7,188,180 filed on March 7, 2014, Petitioner Apple Inc., – Petition for Inter Partes Review, 65 pages	
	D2353	IPR2014-00481; Inter Partes Review of Patent Number 7.188.180 filed on March 7, 2014, Petitioner Apple Inc., – Exhibit 1029: Declaration of Michael Fratto Regarding U.S. Patent Number 7,188,180, 233 pages (2014)	
	D2354	IPR2014-00482; Inter Partes Review of Patent Number 7,188,180 filed on March 7, 2014, Petitioner Apple Inc., – Petition for Inter Partes Review, 68 pages	
	D2355	IPR2014-00482; Inter Partes Review of Patent Number 7.188.180 filed on March 7, 2014, Petitioner Apple Inc., – Exhibit 1029: Declaration of Michael Fratto Regarding U.S. Patent Number 7,188,180, 233 pages (2014)	
	D2356	IPR2014-00483; Inter Partes Review of Patent Number 7,987,274 filed on March 7, 2014, Petitioner Apple Inc., – Petition for Inter Partes Review, 63 pages	
	D2357	IPR2014-00483; Inter Partes Review of Patent Number 7,987,274 filed on March 7, 2014, Petitioner Apple Inc., – Exhibit 1029: Declaration of Michael Fratto Regarding U.S. Patent Number 7,188,180, 191 pages (2014)	
	D2358	IPR2014-00484; Inter Partes Review of Patent Number 7,987,274 filed on March 7, 2014, Petitioner Apple Inc., – Petition for Inter Partes Review, 63 pages	
	D2359	IPR2014-00484; Inter Partes Review of Patent Number 7,987,274 filed on March 7, 2014, Petitioner Apple Inc., – Exhibit 1029: Declaration of Michael Fratto Regarding U.S. Patent 7,987,274, 191 pages (2014)	
	D2360	IPR2014-00485; Inter Partes Review of Patent Number 8,051,181 filed on March 7, 2014, Petitioner Apple Inc., – Petition for Inter Partes Review, 73 pages	
	D2361	IPR2014-00485; Inter Partes Review of Patent Number 8,051,181 filed on March 7, 2014, Petitioner Apple Inc., – Exhibit 1011: Declaration of Dr. Roch Guerin, 24 pages (2014)	
	D2362	IPR2014-00485; Inter Partes Review of Patent Number 8,051,181 filed on March 7, 2014, Petitioner Apple Inc., – Exhibit 1029: Declaration of Michael Fratto, 448 pages (2014)	
	D2363	IPR2014-00485; Inter Partes Review of Patent Number 8,051,181 filed on March 7, 2014, Petitioner Apple Inc., – Exhibit 1014: US District Court Civil Docket 6:10cv94, Virnetx Inc. v. Microsoft Corporation dated August 21, 2013	
	D2364	IPR2014-00485; Inter Partes Review of Patent Number 8,051,181 filed on March 7, 2014, Petitioner Apple Inc., – Exhibit 1083: ITU-T Recommendation H.225.0; Call Signaling Protocols and Media Stream Packetization for Packet-Based Multimedia Communication Systems, Series H: Audiovisual and Multimedia Systems (1998)	
	D2365	IPR2014-00485; Inter Partes Review of Patent Number 8,051,181 filed on March 7, 2014, Petitioner Apple Inc., – Exhibit 1084: ITU-T Recommendation H.235; Security and Encryption for H-Series (H.323 and other H.245-Based) Multimedia Terminals, Series H: Audiovisual and Multimedia Systems (1998)	
	D2366	IPR2014-00485; Inter Partes Review of Patent Number 8,051,181 filed on March 7, 2014, Petitioner Apple Inc., – Exhibit 1085: ITU-T Recommendation H.245;Control Protocol for Multimedia Communication, Series H: Audiovisual and Multimedia Systems (1998)	
	D2367	IPR2014-00485; Inter Partes Review of Patent Number 8,051,181 filed on March 7, 2014, Petitioner Apple Inc., – Exhibit 1070: Joint Claim Construction and Prehearing Statement filed February 14, 2014	
	D2368	IPR2014-00485; Inter Partes Review of Patent Number 8,051,181 filed on March 7, 2014, Petitioner Apple Inc., – Exhibit 1071: Parties' Joint List of Proposed Construction of Remaining Disputed Claim Terms dated 2/25/2013	
	D2369	IPR2014-00486; Inter Partes Review of Patent Number 8,051,181 filed on March 7, 2014, Petitioner Apple Inc., – Petition for Inter Partes Review, 72 pages	
	D2370	IPR2014-00486; Inter Partes Review of Patent Number 8,051,181 filed on March 7, 2014, Petitioner Apple Inc., – Exhibit 1029: Declaration of Michael Fratto, 448 pages (2014)	

/Krisna Lim/ 07/01/2014

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

	D2371	Request for Inter Partes Reexamination of Patent Number 7,490,151 filed on August 16, 2011, Requester Cisco Systems., - Original Petition to Request Inter Partes Reexamination, 210 pages	
	D2372	BinTec Communications AG; Extended Feature Guide, Version 1.2 (1999)	
	D2373	Eagle Integrated Enterprise; Network Security System, 5.0 Reference Guide (1998)	
	D2374	Configuration Guide for the Cisco Secure PIX Firewall Version 5.0; Configuration Forms (1999)	
	D2375	Overview of Access VPNs and Tunneling Technologies, 1998, Cisco Systems, Inc.	
	D2376	Bianca/Brick-XMP; User's Guide – Hardware and Installation, Version 1.3 (1999)	
	D2377	Cisco Multimedia Conference Manager; Provides H.323 Gatekeeper and Proxy Services for Reliable and Scalable Videoconferencing and Voice-over-IP Deployments (1999)	
	D2378	Cisco Multimedia Conference Manager; Release 11.3 (Microsoft Invalidity Contentions Documents dated 3/20/14)	
	D2379	Trial Transcript in *VimetX Inc. v. Apple Inc.*, 6:10-cv-417 (E.D. Tex. Oct. 31, 2012 to Nov. 6, 2012)	
	D2380	VirnetX's Opening Claim Construction Brief, *VimetX Inc. v. Apple Inc.*, 6:11-cv-563, 6:12-cv-855 (E.D. Tex. Mar. 24, 2014)	
	D2381	IPR2014-00558; Inter Partes Review of Patent Number 6,502,135 filed on March 31, 2014, Petitioner Microsoft Corp., – Petition for Inter Partes Review, 56 pages	
	D2382	IPR2014-00558, Ex. 1003, Declaration of Dr. Roch Guerin submitted March 31, 2014 (41 pages)	

EXAMINER /Krisna Lim/	DATE CONSIDERED 07/01/2014

*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./

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13615557	LARSON ET AL.
	Examiner	**Art Unit**
	KRISNA LIM	2453

CPC- SEARCHED

Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED

Symbol	Date	Examiner

US CLASSIFICATION SEARCHED

Class	Subclass	Date	Examiner
709709	222-227222-227	07/25/201305/29 /2013	klkl

SEARCH NOTES

Search Notes	Date	Examiner
InventorsInventors	07/25/201305/2 9/2014	klkl

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
709	222-227	05/29/2014	kl

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13615557	LARSON ET AL.
	Examiner	**Art Unit**
	KRISNA LIM	2453

CPC

Symbol			Type	Version
H04L	63	/ 0428	I	2013-01-01
H04L	29	/ 12066	I	2013-01-01
H04L	61	/ 2092	I	2013-01-01
G06F	21	/ 606	I	2013-01-01
H04L	67	/ 14	F	2013-01-01
H04L	61	/ 6004	I	2013-01-01
H04L	63	/ 1408	I	2013-01-01
H04L	61	/ 303	I	2013-01-01
H04L	29	/ 12301	I	2013-01-01
H04L	63	/ 08	I	2013-01-01
H04L	29	/ 1232	I	2013-01-01
H04L	61	/ 2076	I	2013-01-01
H04L	61	/ 35	I	2013-01-01
H04L	45	/ 28	I	2013-01-01
H04L	29	/ 12801	I	2013-01-01
H04L	29	/ 12783	I	2013-01-01
H04L	63	/ 0407	I	2013-01-01
H04L	63	/ 0227	I	2013-01-01
H04L	45	/ 24	I	2013-01-01
H04L	29	/ 12594	I	2013-01-01
H04L	45	/ 00	I	2013-01-01
H04L	12	/ 4641	I	2013-01-01
H04L	63	/ 1458	I	2013-01-01
H04L	63	/ 105	A	2013-01-01
H04L	29	/ 12216	I	2013-01-01
H04L	63	/ 1416	I	2013-01-01
H04L	41	/ 00	I	2013-01-01
H04L	63	/ 04	I	2013-01-01
H04L	63	/ 1466	I	2013-01-01
H04L	63	/ 164	A	2013-01-01
H04L	61	/ 1511	I	2013-01-01

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 34	
/KRISNA LIM/ Primary Examiner.Art Unit 2453 (Primary Examiner)	07/01/2014 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 26, 27

Issue Classification	**Application/Control No.**	**Applicant(s)/Patent Under Reexamination**
	13615557	LARSON ET AL.
	Examiner	**Art Unit**
	KRISNA LIM	2453

H04L		61	/	2007	I	2013-01-01
H04L		63	/	0272	I	2013-01-01

CPC Combination Sets								
Symbol					**Type**	**Set**	**Ranking**	**Version**
			/					
			/					

NONE (Assistant Examiner) (Date)	**Total Claims Allowed:** 34	
/KRISNA LIM/ Primary Examiner.Art Unit 2453 07/01/2014 (Primary Examiner) (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 26, 27

Issue Classification	**Application/Control No.** 13615557	**Applicant(s)/Patent Under Reexamination** LARSON ET AL.
	Examiner KRISNA LIM	**Art Unit** 2453

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**
709	222

CROSS REFERENCE(S)

CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**				
709	223	223	224	225	226
709	227				

INTERNATIONAL CLASSIFICATION

CLAIMED					**NON-CLAIMED**				
G	0	6	F	15 / 173 (2006.01.01)					

NONE (Assistant Examiner) (Date)	**Total Claims Allowed:** 34	
/KRISNA LIM/ Primary Examiner.Art Unit 2453 07/01/2014 (Primary Examiner) (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 26, 27

Issue Classification	Application/Control No. 13615557	Applicant(s)/Patent Under Reexamination LARSON ET AL.
	Examiner KRISNA LIM	Art Unit 2453

☐ 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
1	1	14	17	16	33										
2	2	15	18	17	34										
	3	21	19	18	35										
3	4	22	20	19	36										
4	5	23	21	20	37										
5	6	24	22												
6	7	25	23												
7	8	26	24												
8	9	27	25												
9	10	28	26												
	11	29	27												
10	12	30	28												
	13	31	29												
11	14	32	30												
12	15	33	31												
13	16	34	32												

NONE (Assistant Examiner)	(Date)	Total Claims Allowed: 34	
/KRISNA LIM/ Primary Examiner.Art Unit 2453 (Primary Examiner)	07/01/2014 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 26, 27

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13615557	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	07/25/2013	11/06/2013	02/19/2014	05/29/2014					
1	1	✓	✓	✓	=					
2	2	✓	✓	✓	=					
	3	✓	-		-					
3	4	✓	✓	✓	=					
4	5	✓	✓	✓	=					
5	6	✓	✓	✓	=					
6	7	✓	✓	✓	=					
7	8	✓	✓	✓	=					
8	9	✓	✓	✓	=					
9	10	✓	✓	✓	=					
	11	✓	-	-	-					
10	12	✓	✓	✓	=					
	13	✓	-	-	-					
11	14	✓	✓	✓	=					
12	15	✓	✓	✓	=					
13	16	✓	✓	✓	=					
14	17	✓	✓	✓	=					
15	18	✓	✓	✓	=					
21	19	✓	✓	✓	=					
22	20	✓	✓	✓	=					
23	21		✓	✓	=					
24	22		✓	✓	=					
25	23		✓	✓	=					
26	24		✓	✓	=					
27	25		✓	✓	=					
28	26		✓	✓	=					
29	27		✓	✓	=					
30	28		✓	✓	=					
31	29		✓	✓	=					
32	30		✓	✓	=					
33	31		✓	✓	=					
34	32		✓	✓	=					
16	33		✓	✓	=					
17	34		✓	✓	=					
18	35		✓	✓	=					
19	36		✓	✓	=					

Index of Claims	Application/Control No. 13615557	Applicant(s)/Patent Under Reexamination LARSON ET AL.
	Examiner KRISNA LIM	Art Unit 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	07/25/2013	11/06/2013	02/19/2014	05/29/2014					
20	37		✓	✓	=					

Docket No.: 077580-0177
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Victor LARSON, *et al.*	:	Customer Number: 23630
Application No.: 13/615,557	:	Confirmation No. 1089
Filed: September 13, 2012	:	Group Art Unit: 2453
For: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES	:	Examiner: Krisna Lim

Mail Stop Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT UNDER 37 C.F.R. § 1.312 AND COMMENTS ON EXAMINER'S STATEMENT OF REASONS FOR ALLOWANCE

Commissioner:

Further to a Notice of Allowance mailed on June 10, 2014 ("Notice of Allowance"), and without withdrawing the application from issue, please enter the following amendments under 37 C.F.R. § 1.312 and remarks.

Amendments to the Claims begin on page 2 of this paper.

Remarks begin on page 8 of this paper.

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows. This listing of the claims replaces all prior listings of the claims.

1. (Currently Amended) A method of transparently creating an encrypted communications channel between a client device and a target device, each device being configured to allow secure data communications between the client device and the target device over the encrypted communications channel once the encrypted communications channel is created, the method comprising:

(1) intercepting from the client device a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device;

(2) determining whether the request to look up the IP address ~~transmitted~~ intercepted in step (1) corresponds to a device that accepts an encrypted channel connection with the client device; and

(3) in response to determining, in step (2), that the request to look up the IP address in step (2) corresponds to a device that accepts an encrypted communications channel connection with the client device, providing provisioning information required to initiate the creation of the encrypted communications channel between the client device and the target device such that the encrypted communications channel supports secure data communications transmitted between the two devices, the client device being a device at which a user accesses the encrypted communications channel.

2. (Previously Presented) The method of claim 1, wherein providing the provisioning information required to initiate the encrypted communications channel is based on a determination that the target device is a device with which an encrypted communications channel can be established when the IP address request corresponds to a target device identified in an network address lookup.

3. (Canceled)

4. (Previously Presented) The method of claim 1, wherein the domain name is a secure domain name.

5. (Original) The method of claim 1, wherein the encrypted communications channel is a broadband connection.

6. (Original) The method of claim 1, wherein the encrypted communications channel is an unmodulated transmission link.

7. (Previously Presented) The method of claim 1, wherein the encrypted communications channel is a modulated transmission link.

8. (Previously Presented) The method of claim 1, wherein the encrypted communications channel supports at least one of the following: FDM, TDM and CDMA.

9. (Original) The method of claim 1, wherein the client device is a phone.

10. (Previously Presented) The method of claim 9, wherein providing the provisioning information required to initiate the encrypted communications channel is based on a determination that the target device is a device with which an encrypted communications channel can be established when the IP address request corresponds to a target device identified in an network address lookup.

11. (Canceled)

12. (Previously Presented) The method of claim 9, wherein the domain name is a secure domain name.

13. (Canceled)

14. (Original) The method of claim 9, wherein the encrypted communications channel is an unmodulated transmission link.

15. (Original) The method of claim 9, wherein the encrypted communications channel is a modulated transmission link.

16. (Previously Presented) The method of claim 9, wherein the encrypted communications channel supports at least one of the following: FDM, TDM and CDMA.

17. (Previously Presented) The method of claim 1, wherein the target device is a server.

18. (Previously Presented) The method of claim 1, wherein the target device is a phone.

19. (Currently Amended) A system for transparently creating an encrypted communications channel between a client device and a target device, each device being configured to allow secure data communications therebetween over an encrypted communications channel once the encrypted communications channel is created, the system including a memory storing instructions, and a server configuration arranged to:

(1) intercept from the client device a request to look up an Internet ~~Protcol~~ Protocol (IP) address corresponding to a domain name associated with the target device;

(2) determine whether the request to look up the IP address ~~transmitted~~ intercepted in step (1) corresponds to a device that accepts an encrypted channel connection with the client device; and

(3) in response to determining, in step (2), that the request to look up the IP address corresponds to a device that accepts an encrypted communications channel connection with the client device, provide provisioning information required to initiate the creation of the encrypted communications channel between the client device and the target device such that the encrypted communications channel supports secure data communications transmitted between the two

devices, the client device being a device at which a user accesses the encrypted communications channel.

20. (Previously Presented) A system according to claim 19, wherein the encrypted communications channel supports a plurality of services.

21. (Previously Presented) The system according to claim 19, wherein the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof.

22. (Previously Presented) The system according to claim 21, wherein the plurality of other application programs comprises at least one of the following: e-mail, a word processing program, and telephony.

23. (Previously Presented) The system according to claim 19, wherein the domain name is a secure domain name.

24. (Previously Presented) The system according to claim 19, wherein the encrypted communications channel is a broadband connection.

25. (Previously Presented) The system according to claim 19, wherein the encrypted communications channel is an unmodulated transmission link.

26. (Previously Presented) The system according to claim 19, wherein the encrypted communications channel is a modulated transmission link.

27. (Previously Presented) The system according to claim 19, wherein the encrypted communications channel supports at least one of the following: FDM, TDM and CDMA.

28. (Previously Presented) The system according to claim 19, wherein the client device is a phone.

29. (Previously Presented) The system according to claim 19, wherein the target device is a server.

30. (Previously Presented) The system according to claim 19, wherein the target device is a phone.

31. (Previously Presented) The system according to claim 19, wherein intercepting the request consists of the system receiving the request to determine whether the target device accepts an encrypted channel connection with the client device.

32. (Previously Presented) The system according to claim 19, wherein intercepting the request occurs within another device that is separate from the client device.

33. (Previously Presented) The method according to claim 1, wherein intercepting the request consists of receiving the request to determine whether the target device accepts an encrypted channel connection with the client device.

34. (Previously Presented) The method according to claim 1, wherein the intercepting the request occurs within another device that is separate from the client device.

35. (Previously Presented) The method according to claim 1, wherein the encrypted communications channel supports a plurality of services.

36. (Previously Presented) The method according to claim 35, wherein the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof.

37. (Previously Presented) The method according to claim 36, wherein the plurality of other application programs comprises at least one of the following: e-mail, a word processing program, and telephony.

REMARKS

Claims 1, 2, 4-10, 12, and 14-37 remain pending in the application and stand allowed, with claims 1 and 19 being the independent claims. Independent claims 1 and 19 are amended to address formal matters relating to self-evident corrections, without changing the scope of the claims. The amendments should be entered under 37 C.F.R. § 1.312 without withdrawing the application from issue. M.P.E.P. § 714.16.

The Notice of Allowance is accompanied by a Notice of Allowability containing a statement of the Examiner's reasons for allowance, which characterizes the allowed claims and cited references (Kiuchi and Wesinger). (*See* Notice of Allowability at 2-3.) Applicants agree with the Examiner's conclusion that the claims are allowable, but do not necessarily agree with the Examiner's characterizations or all of the Examiner's reasoning. For instance, Applicant submits that each of the allowed claims is patentable based on the subject matter defined by the claim language and the combination of recitations within the claims, and not based solely on the recitations highlighted by the Examiner. Additionally, Applicants maintain that the claims are patentable over the cited references for reasons discussed in Applicants' prior responses, not only for the reasons mentioned by the Examiner.

CONCLUSION

Applicants respectfully request entry of the above-discussed amendments to independent claims 1 and 19 under 37 C.F.R. § 1.312 without withdrawing the application from issue, as well as entry of Applicants' above comments on the Examiner's statement of reasons for allowance. If 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 501133, and please credit any excess fees to the deposit account.

The Examiner is encouraged to call the undersigned attorney should he wish to resolve any outstanding issues in connection with the present application.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Date: September 8, 2014

/Toby H. Kusmer/

Toby H. Kusmer, PC
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Reg. No. 26,418
DD Telephone: (617) 535-4065
Fax: (617) 535-3800
E-mail: tkusmer@mwe.com

Electronic Acknowledgement Receipt

EFS ID:	20085502
Application Number:	13615557
International Application Number:	
Confirmation Number:	1089
Title of Invention:	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:	077580-0177
Receipt Date:	09-SEP-2014
Filing Date:	13-SEP-2012
Time Stamp:	14:12:43
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	Amendment after Notice of Allowance (Rule 312)	Amendment.pdf	147725 2a95382469ccb300e10390055de2dc98dfebeb37	no	9

Warnings:

Information:

Total Files Size (in bytes):	147725

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.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

23630 7590 06/10/2014

McDermott Will & Emery
The McDermott Building
500 North Capitol Street, N.W.
Washington, DC 20001

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/615,557	09/13/2012	Victor Larson	077580-0177	1089

TITLE OF INVENTION: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	09/10/2014

EXAMINER	ART UNIT	CLASS-SUBCLASS
LIM, KRISNA	2453	713-162000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
   - ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
   - ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
   (1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
   (2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
   1 McDermott Will & Emery LLP
   2 ____
   3 ____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: VirnetX, Inc.
(B) RESIDENCE: (CITY and STATE OR COUNTRY): Zephyr Cove, NV

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
- ☒ Issue Fee
- ☐ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies ____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ☐ A check is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number 50-1133 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ☐ Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ☐ Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ☐ Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Toby H. Kusmer/ Date September 9, 2014

Typed or printed name Toby H. Kusmer Registration No. 26,418

Electronic Patent Application Fee Transmittal

Application Number:	13615557
Filing Date:	13-Sep-2012
Title of Invention:	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:	077580-0177

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:				
Utility Appl Issue Fee	1501	1	960	960
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
		Total in USD ($)		**960**

Electronic Acknowledgement Receipt

EFS ID:	20091337
Application Number:	13615557
International Application Number:	
Confirmation Number:	1089
Title of Invention:	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:	077580-0177
Receipt Date:	09-SEP-2014
Filing Date:	13-SEP-2012
Time Stamp:	17:44:18
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$960
RAM confirmation Number	2223
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	Issue Fee Payment (PTO-85B)	IssueFeePayment.pdf	87956 b7eb646444654627c350434b74721fad326 20801	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30508 317610be3b79b65877473537a1e53cabf3e 11a5e	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	118464	

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.

OK TO ENTER: /K.L./

09/12/2014

Docket No.: 077580-0177
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Victor LARSON, *et al.*	:	Customer Number: 23630
Application No.: 13/615,557	:	Confirmation No. 1089
Filed: September 13, 2012	:	Group Art Unit: 2453
For: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES	:	Examiner: Krisna Lim

Mail Stop Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT UNDER 37 C.F.R. § 1.312 AND COMMENTS ON EXAMINER'S STATEMENT OF REASONS FOR ALLOWANCE

Commissioner:

Further to a Notice of Allowance mailed on June 10, 2014 ("Notice of Allowance"), and without withdrawing the application from issue, please enter the following amendments under 37 C.F.R. § 1.312 and remarks.

Amendments to the Claims begin on page 2 of this paper.

Remarks begin on page 8 of this paper.

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.
13/615,557	09/13/2012	Victor Larson	077580-0177	1089

23630 7590 09/25/2014

McDermott Will & Emery
The McDermott Building
500 North Capitol Street, N.W.
Washington, DC 20001

EXAMINER	
LIM, KRISNA	
ART UNIT	**PAPER NUMBER**
2453	

NOTIFICATION DATE	DELIVERY MODE
09/25/2014	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

Response to Rule 312 Communication	Application No. 13/615,557	Applicant(s) LARSON ET AL.
	Examiner KRISNA LIM	Art Unit 2453

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address –

1. ☒ The amendment filed on *09 September 2014* under 37 CFR 1.312 has been considered, and has been:

   a) ☒ entered.

   b) ☒ entered as directed to matters of form not affecting the scope of the invention.

   c) ☐ disapproved because the amendment was filed after the payment of the issue fee.
   Any amendment filed after the date the issue fee is paid must be accompanied by a petition under 37 CFR 1.313(c)(1) and the required fee to withdraw the application from issue.

   d) ☐ disapproved. See explanation below.

   e) ☐ entered in part. See explanation below.

/KRISTA ZELE/ Supervisory Patent Examiner, Art Unit 2453	/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	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**077580-0177 (VRNK-0001CP3CON8)**

	D1257	Press Relese; Virnetx and NEC Corporation and NEC Corporation of America Sign a Patent License Agreement, 5 pages, August 2012, Printed from Website: http://virnetx.com/vimetx-and-nec-corporation-and-nec-corporation-of-america-sign-a-patent-license-agreement/	
	D1258	Supplemental Declaration of Angelos D. Keromytis, Ph.D from Control No.: 95001789 pp. 1-18, dated December 20, 2012	
	D1259	Supplemental Declaration of Angelos D. Keromytis, Ph.D from Control No.: 95001851 pp. 1-13, dated December 30, 2012	
	D1260	Supplemental Declaration of Angelos D. Keromytis, Ph.D from Control No.: 95001788 pp. 1-18, dated December 18, 2012	
	D1261	Supplemental Declaration of Angelos D. Keromytis, Ph.D from Control No.: 95001856 pp. 1-13, dated December 30, 2012	
	D1262	VirnetX vs Apple Transcript of Trial, Afternoon Session, 12:05 p.m., dated November 5, 2012	
Change(s) applied to document, /C.C.B./ 8/16/2014	D1263	Certified Copy dated ~~September 18, 2012~~ of U.S. Patent Number 6,502,135, 73 pages 12/2002	Munger et al.
	D1264	Certified Copy dated December 30, 2009 of Assignment for Patent Application Number 95/047,83 12 pages	
	D1265	Certified Copy dated March 11, 2008 of Patent Application Number 09/504,783, 1500 pages	
	D1266	Certified Copy dated ~~March 30, 2011~~ of U.S. Patent Number 7,418,504, 74 pages 08/2008	Larson et al.
	D1267	Certified Copy dated October 17, 2012 of Assignment for Patent Application Number: 10/714,849, 10 pages	
	D1268	Certified Copy dated April 4, 2011 of Patent Application Number 10/714,849, 1170 pages	
	D1269	Certified Copy dated ~~March 30, 2011~~ of U.S. Patent Number 7,490,151, 63 pages 02/2009 Munger et al.	
	D1270	Certified Copy dated October 17, 2012 of Assignment for Patent Application Number 10/259,494, 19 pages	
	D1271	Certified Copy dated April 4, 2011 of Application Number 10/259,454, 1359 pages	
	D1272	Certified Copy dated April 12, 2011 of U.S. Patent Number 7,921,211, 78 pages Larson et al.	
	D1273	Certified Copy dated October 17, 2012 of Assignment for Application Number 11/840,560, 12 pages	
	D1274	Certified Copy dated April 20, 2011 of Application Number 11/840,560, 3 pages	
	D1275	iPhone User Guide for iPhone OS 3.1 Software, 217 pages, 2009	
	D1276	iPhone User Guide for iOS 4.2 and 4.3 Software, 274 pages, 2011	
	D1277	iPhone User Guide for iPhone and iPhone 3G, 154 pages, 2008	
	D1278	iPhone User Guide for iOS 5.0 Software, 163 pages, 2011	
	D1279	iPad User Guide for iOS 5.0 Software, 141 pages, 2011	
	D1280	iPad User Guide for iOS 4.2 Software, 181 pages, 2010	
	D1281	iPad User Guide for iOS 4.3 Software, 198 pages, 2011	
	D1282	iPad User Guide, 154 pages, 2010	
	D1283	iPod Touch User Guide for iOS 5.0 Software, 143 pages, 2011	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

13615557 - GAU: 2453

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT VS. APPLICANT *(Use as many sheets as necessary)*	Application Number	**13/615,557**
	Filing Date	**09-13-2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Krisna Lim**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

OPAP MAY 27 2014 AKIMA-13 PATENT & TRADEMARK OFFICE

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
	A179	RE39,360	10/17/2006	Aziz et al.	
	A180	5,416,842	05/16/1995	Aziz	
	A181	5,420,926	05/30/1995	Low et al.	
	A182	5,444,782	08/22/1995	Adams, Jr. et al.	
	A183	5,455,861	10/03/1995	Faucher et al.	
	A184	5,530,758	06/25/1996	Marino, Jr. et al.	
	A185	5,623,601	04/22/1997	Vu	
	A186	5,636,139	06/03/1997	McLaughlin et al.	
	A187	5,689,566	11/18/1997	Nguyen	
	A188	5,781,550	07/14/1998	Templin et al.	
	A189	5,805,820	09/08/1998	Bellovin et al.	
	A190	5,812,670	09/22/1998	Micali	
	A191	5,884,270	03/16/1999	Walker et al.	
	A192	5,889,863	03/30/1999	Weber	
	A193	5,915,087	06/22/1999	Hammond et al.	
	A194	5,940,393	08/17/1999	Duree et al.	
	A195	5,961,593	10/05/1999	Gabber et al.	
	A196	5,974,454	10/26/1999	Apfel et al.	
	A197	6,003,084	12/14/1999	Green et al.	
Change(s) applied to document, /C.C.B./ 8/19/2014	A198	6,012,088	~~08/04/2000~~	Li et al.	01/2000
	A199	6,016,504	01/18/2000	Arnold et al.	
	A200	6,023,510	02/08/2000	Epstein	
	A201	6,032,118	02/29/2000	Tello et al.	
	A202	6,055,236	04/25/200	Nessett et al.	
	A203	6,055,518	04/25/2000	Franklin et al.	
	A204	6,055,575	04/25/2000	Paulsen et al.	
	A205	6,073,175	06/06/2000	Tavs et al.	
	A206	6,111,883	08/29/2000	Terada et al.	
	A207	6,148,342	11/14/2000	Ho	
	A208	6,151,628	11/21/2000	Xu et al.	
	A209	6,154,839	11/28/2000	Arrow et al.	
	A210	6,182,072	01/30/2001	Leak et al.	
	A211	6,182,141	01/30/2001	Blum et al.	
Change(s) applied to document, /D.D./ 8/9/2014	A212	~~6,199,122~~	03/06/2001	Wilson	6,199,112
	A213	6,225,993	05/01/2001	Lindblad et al.	
	A214	6,298,383	10/02/2001	Gutman et al.	
	A215	6,345,361	02/05/2002	Jerger et al.	

/Krisna Lim/ 07/01/2014

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	**13/615,557**
	Filing Date	**September 13, 2012**
	First Named Inventor	**Victor Larson**
	Art Unit	**2431**
	Examiner Name	**Not Yet Assigned**
	Docket Number	**77580-177 (VRNK-0001CP3CON8)**

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.	08/2009

Change(s) applied to document,
/C.C.B./
8/19/2014

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	**13/615,557**
Filing Dates	**September 13, 2012**
First Named Inventor	**Victor Larson**
Art Unit	**2431**
Examiner Name	**Not Yet Assigned**
Docket Number	**77580-177 (VRNK-0001CP3CON8)**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication/Patent Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A104	6,311,207	10/30/2001	Mighdoll et al	
	A105	6,314,463	11/2001	Abbott et al.	
	A106	6,324,161	11/27/2001	Kirch	
	A107	6,330,562	12/11/2001	Boden et al.	
	A108	6,332,158	12/18/2001	Risley et al.	
	A109	6,333,272	12/25/01	McMillin, et al.	
	A110	6,338,082	01/08/02	Schneider, Eric	
	A111	6,353,614	03/05/2002	Borella et al.	
	A112	6,425,003	07/23/2002	Herzog et al.	
	A113	6,430,155	08/06/2002	Davie et al	
	A114	6,430,610	08/06/2002	Carter	
	A115	6,487,598	11/26/2002	Valencia	
	A116	6,496,867	12/17/2002	Beser et al.	
	A117	6,499,108	12/24/2002	Johnson	
	A118	6,502,135	12/2002	Munger et al.	
	A119	6,505,232	01/07/2003	Mighdoll et al	
	A120	6,510,154	01/21/2003	Mayes et al	
	A121	6,549,516	04/15/2003	Albert et al	
	A122	6,557,037	04/2003	Provino, Joseph E.	
	A123	6,560,634	05/06/2003	Broadhurst	
	A124	6,571,296	~~05/27/2002~~	Dillon	05/2003
	A125	6,571,338	05/27/2003	Shaio et al.	
	A126	6,581,166	~~7/17/2003~~	Hirst et al.	June 17, 2003
	A127	6,606,708	08/12/2003	Devine et al.	
	A128	6,615,357	9/2/2003	Boden et al.	
	A129	6,618,761	09/09/2003	Munger et al.	
	A130	6,671,702	12/30/2003	Kruglikov et al	
	A131	6,687,551	2/3/2004	Steindl	
	A132	6,687,746	02/03/04	Shuster, et al.	
	A133	6,701,437	03/02/2004	Hoke et al.	
	A134	6,714,970	3/30/2004	Fiveash et al.	
	A135	6,717,949	4/6/2004	Boden et al.	
	A136	6,751,738	06/15/2004	Wesinger, Jr. et al..	
	A137	6,752,166	06/22/04	Lull, et al.	
	A138	6,757,740	06/29/04	Parekh, et al.	
	A139	6,760,766	7/6/2004	Sahlqvist	
	A140	6,813,777	11/2004	Weinberger et al.	
	A141	6,826,616	11/30/2004	Larson et al.	
	A142	6,839,759	1/4/2005	Larson et al.	
	A143	6,937,597	08/30/2005	Rosenberg et al.	
	A144	7,010,604	3/7/2006	Munger et al.	
	A145	7,039,713	05/2006	Van Gunter et al.	
	A146	7,072,964	07/04/2006	Whittle et al.	
	A147	7,133,930	11/7/2006	Munger et al.	
	A148	7,167,904	01/23/07	Devarajan, et al.	
	A149	7,188,175	03/06/07	McKeeth, James A.	
	A150	7,188,180	3/6/2007	Larson et al.	
	A151	7,197,563	3/27/2007	Sheymov et al.	
	A152	7,353,841	04/08/08	Kono, et al.	
	A153	7,418,504	08/2008	Larson et al.	
	A154	7,461,334	12/02/08	Lu, et al.	
	A155	7,490,151	02/2009	Munger et al.	

Change(s) applied to document, /C.C.B./ 8/19/2014

Change(s) applied to document, /D.D/ 8/9/2014

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	13/615,557
Filing Dates	September 13, 2012
First Named Inventor	Victor Larson
Art Unit	2431
Examiner Name	Not Yet Assigned
Docket Number	77580-177 (VRNK-0001CP3CON8)

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication/Patent Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1	09/399,753	09/22/1998	Graig Miller et al.	
	A2	60/151,563	08/31/1999	Bryan Whittles	
	A3	60/134,547	05/17/1999	Victory Sheymov	
	A4	2,895,502	07/21/1959	Roper et al.	
	A5	4,761,334	08/1988	Sagoi et al.	
	A6	4,885,778	12/5/1989	Weiss, Kenneth	
	A7	4,920,484	4/24/1990	Ranade	
	A8	4,933,846	06/12/1990	Humphrey et al.	
	A9	4,952,930	08/28/1990	Franaszek et al.	
	A10	4,988,990	01/29/1991	Warrior	
	A11	5,164,988	11/17/1992	Matyas	
	A12	5,204,961	04/20/1993	Barlow	
	A13	5,276,735	01/04/1994	Boebert et al	
	A14	5,303,302	04/12/1994	Burrows	
	A15	5,311,593	05/10/1994	Carmi	
	A16	5,329,521	07/12/1994	Walsh et al.	
	A17	5,341,426	08/23/1994	Barney et al.	
	A18	5,367,643	11/22/1994	Chang et al	
	A19	5,384,848	01/24/1995	Kikuchi	
	A20	5,511,122	04/23/1996	Atkinson	
	A21	5,548,646	08/20/1996	Aziz et al.	
	A22	5,559,883	09/24/1996	Williams	
	A23	5,561,669	10/01/1996	Lenney et al	
	A24	5,588,060	12/24/1996	Aziz	
	A25	5,590,285	12/31/1996	Krause et al.	
	A26	5,625,626	04/29/1997	Umekita	
	A27	5,629,984	05/13/1997	McManis	
	A28	5,654,695	08/05/1997	Olnowich et al	
	A29	5,682,480	10/28/1997	Nakagawa	
	A30	5,689,566	11/18/1997	Nguyen	
	A31	5,689,641	11/18/1997	Ludwig et al.	
	A32	5,740,375	04/14/1998	Dunne et al.	
	A33	5,757,925	05/1998	Faybishenko	
	A34	5,764,906	06/1998	Edelstein et al.	
	A35	5,771,239	06/23/1998	Moroney et al.	
	A36	5,774,660	6/30/1998	Brendel et al	
	A37	5,787,172	07/28/1998	Arnold	
	A38	5,790,548	08/04/1998	~~Sitaraman et al.~~	Sistanizadeh, et al.
	A39	5,796,942	08/18/1998	Esbensen	
	A40	5,805,801	09/08/1998	Holloway et al.	
	A41	5,805,803	09/08/1998	Birrell et al.	
	A42	5,822,434	10/13/1998	Caronni et al.	
	A43	5,842,040	11/24/1998	Hughes et al.	
	A44	5,845,091	12/01/1998	Dunne et al.	
	A45	5,864,666	01/1999	Shrader, Theodore Jack London	
	A46	5,867,650	~~02/02/1998~~	Osterman	02/1999
	A47	5,870,610	02/09/1999	Beyda et al.	
	A48	5,878,231	~~05/02/1999~~	Baehr et al	March 2, 1999
	A49	5,892,903	04/06/1999	Klaus	
	A50	5,898,830	04/27/1999	Wesinger, Jr. et al.	
	A51	5,905,859	05/18/1999	Holloway et al.	

Change(s) applied to document, /D.D./ 8/12/2014

Change(s) applied to document, /C.C.B./ 8/19/2014

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	**13/615,557**
Filing Date	**09-13-2012**
First Named Inventor	**Victor Larson**
Art Unit	**2453**
Examiner Name	**Krisna Lim**
Docket Number	**077580-0177 (VRNK-0001CP3CON8)**

	D1383	Spindler et al., "Endogenous Bargaining Power in Bilateral Monopoly and Bilateral Exchange," Canadian Journal of Economics-Revue Canadienne D Economie, pages 464-474, 1974	
	D1384	Myerson, "Game Theory; Analysis or Conflict," Harvard University Press, pages 375-392	
	D1385	Binmore, "The Nash Bargaining Solution in Economic Modelling," The Rand Journal of Economics, 17:176-188, 1996	
	D1386	Rubinstein et al., "On the Interpretation of the Nash Bargaining Solution and its Extension to Non-Expected Utility Preferences," Econometrica, 60:1171-1186, 1992	
	D1387	Greenleaf et al., "Guarantees in Auctions: The Auction House as Negotiator and Managerial Decision Maker," Management Science, 39:1130-1145, 1993	
	D1388	Chan, "Trade Negotiations in a Nash Bargaining Model," Journal of International Economics, 25:253-363, 1987	
	D1389	Lemley et al., "Patent Holdup and Royalty Stacking," Texas Law Review, 85:1991-2049	
	D1390	Cauley, "Winning the Patent Damages Case; A Litigator's Guide to Economic Models and Other Damage Strategies," Oxford Press, pages 29-30, 2044	
	D1391	Degnan et al., "A Survey of Licensed Royalties," Les Nouvelles, pages 91, 93, 94, 1997	
	D1392	Kahn, "The Review of Economics and Statistics," pages 157-164, 1993	
	D1393	Microsoft Company Information; Including Stocks and Financial Information, 83 pages	
	D1394	Apple Press Info: Apple Updates MacBook Pro with Next Generation Processors, Graphics & Thunderbolt I/O Technology, 3 pages, Printed from Website: http://www.apple.com/pr/library/2011/02/24Apple-Updates-MacBook-Pro-with-Next-Generation-Processors-Graphics-Thunderbolt-I-O-Technology.html	
	D1395	Apple Press Info: Apple to Ship Mac OS X Snow Leopard on August 28, 2 pages, Printed from the Website: http://www.apple.com/pr/library/2009/08/24/apple-to-ship-mac-os-x	
	D1396	iPad, Facetime; "Once Again, iPad gets the World Talking," 3 pages, Printed from the Website: http://www.apple.com/ipad/built-in-apps/facetime/html	
	D1397	Apple iOS: Setting up VPN, 2 pages, Printed from Website: http/support.apple.com/kb/HT1424	
	D1398	Apple iPhone User Guide for iOS 5.1 Software, 179 pages, 2012	
	D1399	Apple, Communicating with HTTP Servers, CFNetworking Programming Guide, 6 pages, 2011, Printed from the Website: https://developer.apple.com/library/ios/documentation/networking/conceptual/CFNetwork/CFHT	
	D1400	VirnetX, Gabriel Connection Technology ™ White Paper, 7 pages, 2012	
	D1401	VirnetX, Technology, 4 pages, 2012	
Change(s) applied	D1402	Certified Copy dated ~~January 15, 2008~~ of U.S. Patent Number 6,502,135, 64 pages 12/2002	Munger et al.
to document,	D1403	Inter Partes Reexamination Certificate dated June 7, 2011 for Patent Number 6,502,135	
/C.C.B./	D1404	Proceedings of The Symposium on Network and Distributed System Security, 7 pages, February 22-23, 1996	
8/19/2014	D1405	In-Q-Tel; Corporate Overview, 2 pages, 2004	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

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.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/615,557	10/21/2014	8868705	077580-0177	1089

23630 7590 10/01/2014

McDermott Will & Emery
The McDermott Building
500 North Capitol Street, N.W.
Washington, DC 20001

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

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