

UTILITY PATENT APPLICATION TRANSMITTAL (Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
77580-066 (VRNK-1CP2DVCN2)

Total Pages in this Submission

COMMISSIONER FOR PATENTS

P.O. Box 1450
Alexandria, VA 22313-1450

Transmitted herewith for filing under 35 U.S.C. 111(a) and 37 C.F.R. 1.53(b) is a new utility patent application for an invention entitled:

METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

and invented by:

Victor Larson, Robert Dunham Short III, Edmund Colby Munger and Michael Williamson

If a **CONTINUATION APPLICATION**, check appropriate box and supply the requisite information:

Continuation **Divisional** **Continuation-in-part (CIP)** of prior application No.: 11/679,416

Which is a:

Continuation **Divisional** **Continuation-in-part (CIP)** of prior application No.: 10/702,486

Which is a:

Continuation **Divisional** **Continuation-in-part (CIP)** of prior application No.: 09/558,209

Enclosed are:

Application Elements

1. Filing fee as calculated and transmitted as described below
2. Specification having 78 pages and including the following:
 - a. Descriptive Title of the Invention
 - b. Cross References to Related Applications (if applicable)
 - c. Statement Regarding Federally-sponsored Research/Development (if applicable)
 - d. Reference to Sequence Listing, a Table, or a Computer Program Listing Appendix
 - e. Background of the Invention
 - f. Brief Summary of the Invention
 - g. Brief Description of the Drawings (if filed)
 - h. Detailed Description
 - i. Claim(s) as Classified Below
 - j. Abstract of the Disclosure

**UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)**

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
77580-066 (VRNK-1CP2DVCN2)

Total Pages in this Submission

Application Elements (Continued)

3. Drawing(s) *(when necessary as prescribed by 35 USC 113)*
- a. Formal Number of Sheets 40
- b. Informal Number of Sheets _____
4. Oath or Declaration
- a. Newly executed *(original or copy)* Unexecuted
- b. Copy from a prior application (37 CFR 1.63(d)) *(for continuation/divisional application only)*
- c. With Power of Attorney Without Power of Attorney
- d. DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s) named in the prior application,
see 37 C.F.R. 1.63(d)(2) and 1.33(b).
5. Incorporation By Reference *(usable if Box 4b is checked)*
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.
6. CD ROM or CD-R in duplicate, large table or Computer Program (Appendix)
7. Application Data Sheet (See 37 CFR 1.76)
8. Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all must be included)*
- a. Computer Readable Form (CRF)
- b. Specification Sequence Listing on:
- i. CD-ROM or CD-R (2 copies); or
- ii. Paper
- c. Statement(s) Verifying Identical Paper and Computer Readable Copy

Accompanying Application Parts

9. Assignment Papers *(cover sheet & document(s))*
10. 37 CFR 3.73(B) Statement *(when there is an assignee)*
11. English Translation Document *(if applicable)*
12. Information Disclosure Statement/PTO-1449 Copies of IDS Citations
13. Preliminary Amendment
14. Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
15. Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
16. Certificate of Mailing
- First Class Express Mail *(Specify Label No.):* _____

**UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)**

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
77580-066 (VRNK-1CP2DVCN2)

Total Pages in this Submission

Accompanying Application Parts (Continued)

17. Additional Enclosures *(please identify below):*

Request That Application Not Be Published Pursuant To 35 U.S.C. 122(b)(2)

18. Pursuant to 35 U.S.C. 122(b)(2), Applicant hereby requests that this patent application not be published pursuant to 35 U.S.C. 122(b)(1). Applicant hereby certifies that the invention disclosed in this 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 of applications 18 months after filing of the application.

Warning

An applicant who makes a request not to publish, but who subsequently files in a foreign country or under a multilateral international agreement specified in 35 U.S.C. 122(b)(2)(B)(i), must notify the Director of such filing not later than 45 days after the date of the filing of such foreign or international application. A failure of the applicant to provide such notice within the prescribed period shall result in the application being regarded as abandoned, unless it is shown to the satisfaction of the Director that the delay in submitting the notice was unintentional.

19. Other:

**UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)**

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
77580-066 (VRNK-1CP2DVCN2)

Total Pages in this Submission

Fee Calculation and Transmittal

CLAIMS AS FILED						Fee
For	#Filed	#Allowed	#Extra	Rate		
Total Claims	1	- 20 =	0	x	\$50.00	\$0.00
Indep. Claims	1	- 3 =	0	x	\$200.00	\$0.00
Multiple Dependent Claims (check if applicable) <input type="checkbox"/>						\$0.00
Total # of Pages in Specification		78	Total # of Drawing Sheets		40	
Total # of Sheets	118	Application Size Fee				\$250.00
						Basic Fee
						\$300.00
						Search Fee
						\$500.00
						Examination Fee
						\$200.00
OTHER FEE (specify purpose)						\$0.00
TOTAL FILING FEE						\$1,250.00

- A check in the amount of _____ to cover the filing fee is enclosed.
- The Director is hereby authorized to charge and credit Deposit Account No. **501133** as described below.
- Charge the amount of **\$1,250.00** as filing fee.
 - Credit any overpayment.
 - Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.
 - Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).

Payment by credit card. Form PTO-2038 is attached.

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.

Dated: 8/16/07



Signature

Toby H. Kusmer, P.C.
Reg. No. 26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Telephone: 617.535.4065
Facsimile: 617.535.3800
e-mail: tkusmer@mwe.com

Customer Number: 23630

cc:

ADS

Application Information	
Application Number::	not assigned
Filing Date::	August 16, 2007
Application Type::	Continuation
Subject Matter::	Utility
Suggested Classification	
Suggested Group Art Unit	
CD-ROM or CD-R	
Number of CD Disks	
Number of copies of CDs	
Sequence Submission	
Computer Readable Form (CRF)	
Number of copies of CRF	
Title::	Method For Establishing Secure Communication Link Between Computers Of Virtual Private Network
Attorney Docket Number::	077580-0066 (VRNK-1CP2DVCN2)
Request for Early Publication::	No
Request for Non-Publication::	No
Suggested Drawing Figure::	1
Total Drawing Sheets::	40
Small Entity::	No
Latin Name	
Variety Denomination Name	
Petition Included::	
Petition Type::	
Licensed US Govt. Agency::	
Contract or Grant Numbers::	
Secrecy Order in Parent Appl.::	

Applicant Information	
Applicant Authority Type::	Inventor 1
Primary Citizenship Country::	U.S.
Status::	Full Capacity
Given Name::	Victor
Middle Name::	
Family Name::	Larson
Name Suffix::	
City of Residence::	Fairfax

State or Province of Residence::	VA
Country of Residence::	U.S.
Street of mailing address::	12026 Lisa Marie Court
City of mailing address::	Fairfax
State or Province of mailing address::	VA
Country of mailing address::	U.S.
Postal or Zip Code of mailing address::	22033
Applicant Authority Type::	Inventor 2
Primary Citizenship Country::	U.S.
Status::	Full Capacity
Given Name::	Robert
Middle Name::	Dunham
Family Name::	Short
Name Suffix::	III
City of Residence::	Leesburg
State or Province of Residence::	VA
Country of Residence::	U.S.
Street of mailing address::	38710 Goose Creek Lane
City of mailing address::	Leesburg
State or Province of mailing address::	VA
Country of mailing address::	U.S.
Postal or Zip Code of mailing address::	20175
Applicant Authority Type::	Inventor 3
Primary Citizenship Country::	U.S.
Status::	Full Capacity
Given Name::	Edmund
Middle Name::	Colby
Family Name::	Munger
Name Suffix::	
City of Residence::	Crownsville
State or Province of Residence::	MD
Country of Residence::	U.S.
Street of mailing address::	1101 Opaca Court
City of mailing address::	Crownsville
State or Province of mailing address::	MD
Country of mailing address::	U.S.
Postal or Zip Code of mailing address::	21032

Applicant Authority Type	Inventor 4
Primary Citizenship Country	U.S.
Status	Full Capacity
Given Name	Michael
Middle Name	
Family Name	Williamson
Name Suffix	
City of Residence	South Riding
State or Province of Residence	VA
Country of Residence	U.S.
Street of Mailing Address	26203 Ocala Circle
City of Mailing Address	South Riding
State or Province of Mailing Address	VA
Country of Mailing Address	U.S.
Postal or Zip Code of Mailing Address	20152

Correspondence Information

Correspondence Customer Number:: 23630

Representative Information

Representative Customer Number:: 23630

Domestic Priority Information

Application::	Continuity Type::	Parent Application::	Parent Filing Date::
This application	is a continuation of	11/679,416	February 27, 2007
11/679,416	is a continuation of	10/702,486	November 7, 2003
10/702,486	is a divisional of	09/558,209	April 26, 2000
09/558,209	is a continuation-in-part of	09/504,783	February 15, 2000
09/504,783	is a continuation-in-part of	09/429,643	October 29, 1999
09/429,643	claims the benefit under 35 U.S.C. 119(e) to	60/106,261	October 30, 1998
09/429,643	claims the benefit under 35 U.S.C. 119(e) to	60/137,704	June 7, 1999

Foreign Priority Information

Country::	Application number::	Filing Date::	Priority Claimed::

Assignee Information	
Assignee Name::	VirnetX, Inc.
Street of mailing address::	5615 Scotts Valley Drive, Suite 110
City of mailing address::	Scotts Valley
State or Province of mailing address::	CA
Country of mailing address::	U.S.
Postal or Zip Code of mailing address::	95066

**METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN
COMPUTERS OF VIRTUAL PRIVATE NETWORK**

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority from and is a continuation of co-pending U.S. application serial number 11/679,416, filed February 27, 2007, which is a continuation of U.S. application serial number 10/702,486, filed November 7, 2003, now U.S. Patent No. 7,188,180, issued March 06, 2007, which is a divisional patent application of U.S. application serial number 09/558,209, filed April 26, 2000, now abandoned, which is a continuation-in-part patent application of previously-filed U.S. application serial number 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 serial number 09/429,643, filed on October 29, 1999, now U.S. Patent No. 7,010,604, issued March 03, 2006. The subject matter of U.S. application serial number 09/429,643, which is bodily incorporated herein, derives from provisional U.S. application numbers 60/106,261 (filed October 30, 1998) and 60/137,704 (filed June 7, 1999). The present application is also related to U.S. application serial number 09/558,210, filed April 26, 2000, now abandoned, and which is incorporated by reference herein.

BACKGROUND OF THE INVENTION

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

from knowing which websites or other Internet resources they are “visiting.” These two security issues may be called data security and anonymity, respectively.

[0003] Data security is usually tackled using some form of data encryption. An encryption key *k* 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 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_1 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 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, .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 IP_C . The IP address of a TARP router, however, may not remain constant. To avoid and manage attacks, each TARP router, independently or under direction from another TARP terminal or router, may change its IP address. A separate, unchangeable identifier or address is also defined. This address, called the TARP address, is known only to TARP routers and terminals and may be correlated at any time by a TARP router or a TARP terminal using a Lookup Table (LUT). When a TARP router or terminal changes its IP address, it updates the other TARP routers and terminals which in turn update their respective LUTs. In reality, whenever a TARP router looks up the address of a destination in the encrypted header, it must convert a TARP address to a real IP address using its LUT.

[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 IP_T are formed. The TARP headers IP_T can be identical to normal IP headers or customized in some way. In a preferred embodiment, the TARP headers IP_T are IP headers with added data providing the following information required for routing and reconstruction of messages, some of which data is ordinarily, or capable of being, contained in normal IP headers:

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

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

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

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

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

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

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

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

[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 (fishbowed) 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.
- S10. The TARP packet is encrypted using the memorized link key.
- S11. An IP header is added to the packet that contains the stored IP address, the encrypted TARP packet wrapped with an IP header, and the completed packet transmitted to the next hop or destination.

[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 within 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 IP 1 and IP2, while a second Ethernet frame 1160 comprises a different frame header 1104 and a single IP packet IP3. Each frame header generally includes a source hardware address 1101A and a destination hardware address 1101B; other well-known fields in frame headers are omitted from FIG. 11 for clarity. Two hardware nodes communicating over a physical communication channel insert appropriate source and destination hardware addresses to indicate which nodes on the channel or network should receive the frame.

[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 1221X, and node 1201 maintains a matching receive table 1209 using the same algorithm 1209X. As node 1202 transmits packets to node 1201 using seemingly random IP source, IP destination, and/or discriminator fields, node 1201 matches the incoming packet values to those falling within window 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 1101B in FIG. 11) that are synchronized to a corresponding receive table 1224 at node 1202. Similarly, node 1202 maintains a different transmit table 1223 containing source and destination hardware addresses that is synchronized with a corresponding receive table 1211 at node 1201. In this manner, outgoing hardware frames appear to be originating from and going to completely random nodes on the network, even though each recipient can determine whether a given packet is intended for it or not. It will be appreciated that the hardware hopping feature can be implemented at a different level in the communications protocol than the IP hopping feature (e.g., in a card driver or in a hardware card itself to improve performance).

[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 it 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).

[00148] 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.

[00149] 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.

[00150] 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).

[00151] 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.

[00152] 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

[00153] 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.

[00154] 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 $X_1, X_2, X_3 \dots X_k$ starting with seed X_0 using a recurrence

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

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

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

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

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

It can be shown that:

$$\begin{aligned} & (a^i (X_0(a-1)+b)-b)/(a-1) \bmod c = \\ & ((a^i \bmod ((a-1)c)(X_0(a-1)+b) - b)/(a-1)) \bmod c. \end{aligned} \quad (4)$$

$(X_0(a-1)+b)$ can be stored as $(X_0(a-1)+b) \bmod c$, b as $b \bmod c$ 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

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

to generate the random number for the $j+1^{\text{th}}$ 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).

[00156] 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.

[00157] 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

[00158] Consider a RNG where $a=31, b=4$ and $c=15$. For this case equation (1) becomes:

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

[00159] 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 $a^n \text{ mod } ((a-1)c) = 31^3 \text{ mod } (15*30) = 29791 \text{ mod } (450) = 91$. Equation (5) becomes:

$$((91 (X_i * 30 + 4) - 4) / 30) \text{ mod } 15 \quad (7).$$

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

TABLE 1

I	X_i	$(X_i * 30 + 4)$	$91 (X_i * 30 + 4) - 4$	$((91 (X_i * 30 + 4) - 4) / 30)$	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:

1. The addresses have no validity outside of the Ethernet and will not be routed out to a valid outside destination by a gateway.
2. There are 2^{24} (~16 million) addresses that can be hopped within each “A” block. This yields >280 trillion possible address pairs making it very unlikely that an adversary would guess a valid address. It also provides acceptably low probability of collision between separate VPNs (all VPNs on a shared medium independently generate random address pairs from the same “A” block).
3. The packets will not be received by someone on the Ethernet who is not on a VPN (unless the machine is in promiscuous mode) minimizing impact on non-VPN computers.

[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 135th bit of the vector would be set. Consequently, one could very quickly determine whether an address of 135 was valid by checking only one bit: the 135th bit. The

presence vectors could be created in advance corresponding to the table entries for the IP addresses. In effect, the incoming addresses can be used as indices into a long vector, making comparisons very fast. As each RNG generates a new address, the presence vector is updated to reflect the information. As the window moves, the presence vector is updated to zero out addresses that are no longer valid.

[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 $2 \times \text{WINDOW_SIZE} + \text{OoO}$ active addresses ($1 \leq \text{OoO} \leq \text{WINDOW_SIZE}$ and $\text{WINDOW_SIZE} \geq 1$) OoO and WINDOW_SIZE are engineerable parameters, where OoO is the minimum number of addresses needed to accommodate lost packets due to events in the network or out of order arrivals and WINDOW_SIZE is the number of packets transmitted before a SYNC_REQ is issued. FIG. 17 depicts a storage array for a receiver’s active addresses.

[00170] The receiver starts with the first $2 \times \text{WINDOW_SIZE}$ addresses loaded and active (ready to receive data). As packets are received, the corresponding entries are marked as “used” and are no longer eligible to receive packets. The transmitter maintains a packet counter, initially set to 0, containing the number of data packets transmitted since the last *initial* transmission of a SYNC_REQ for which SYNC_ACK has been received. When the transmitter packet counter equals WINDOW_SIZE, the transmitter generates a SYNC_REQ and does its initial transmission. When the receiver receives a SYNC_REQ corresponding to its current CKPT_N, it generates the next WINDOW_SIZE addresses and starts loading them in order starting at the first location after the last active address wrapping around to the beginning of the array after the end of the array has been reached. The receiver’s array might look like FIG. 18 when a SYNC_REQ has been received. In this case a couple of packets have been either lost or will be received out of order when the SYNC_REQ is received.

[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 $2 \times \text{WINDOW_SIZE} - \text{OoO}$ then the transmitter ceases sending data packets until the appropriate SYNC_ACK is finally received. The transmitter then resumes sending data packets. Future behavior is essentially a repetition of this initial cycle. The advantages of this approach are:

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

2. No packet is ever transmitted that does not have a corresponding entry in the receiver side
3. No timer based re-synchronization is necessary. This is a consequence of 2.
4. The receiver will always have the ability to accept data messages transmitted within OoO messages of the most recently transmitted message.

J. Distributed Transmission Path Variant

[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 X1. A similar regime holds true for the other paths as shown. Initially, each link's weight value can be set such that it is proportional to its bandwidth, which will be referred to as its "steady-state" value.

[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 assess 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:

$$P' = \alpha \times \text{MIN} + (1 - \alpha) \times P \quad (1)$$

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

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

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

where β is a parameter such that $0 \leq \beta \leq 1$ 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, $\alpha=.75$ and $\beta=.5$. 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 L3's traffic weight value would be set to 0.25.

3. Link L1 finally received a SYNC_ACK containing a MESS_R of 0 indicating that none of the MESS_T (32) messages transmitted in the last window were successfully received. Link L1 would be below THRESH. Link L1's traffic weight value would be increased to .005, link L2's traffic weight value would be decreased to 0.74625, and link L3's traffic weight value would be decreased to 0.24875.

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

5. Link L1 received a SYNC_ACK containing a MESS_R of 32 indicating that 100% of the MESS_T (32) messages transmitted in the last window were successfully received.

Link L1 would be above THRESH. Link L1 's traffic weight value would be increased to 0.37625; link L2's traffic weight value would be decreased to 0.4678125, and link L3's traffic weight value would be decreased to 0.1559375.

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

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

[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 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.

[00207] 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.

[00208] 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

[00209] 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.

[00210] 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.

[00211] 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.

[00212] 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 $M \times N \times W / R$ 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.

[00213] Two practical issues should be considered when implementing the above scheme:

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

[00214] 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.

[00215] 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.

[00216] 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).

[00217] 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.

[00218] 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

[00219] 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.

[00220] 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.

[00221] 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.

[00222] 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.

[00223] 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.

[00224] 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.

[00225] 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.

[00226] 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.

[00227] 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.

[00228] 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.

[00229] 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.

[00230] Assuming that a client application wishes to send a packet to the server on the client’s standing signaling VPL:

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

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

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

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

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

5. When the server receives a SYNC_REQ on its CKPT_N, it replaces its CKPT_O with CKPT_N and generates the next CKPT_N. It updates its transmitter side CKPT_R to correspond to the client's receiver side CKPT_R and transmits a SYNC_ACK containing CKPT_O in its payload.

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

[00231] 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 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.

[00232] 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 a new CKPT_R in the server side transmitter and transmits a SYNC_ACK containing the server side receiver's CKPT_O to 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.

[00233] 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.

[00234] 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

[00235] 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.

[00236] 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.

[00237] 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.

[00238] 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.”

[00239] 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.

[00240] 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.

[00241] 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.

[00242] 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.

[00243] 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.

[00244] 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.

[00245] 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 .com server address for a secure server 3320 corresponding to server 3304.

[00246] 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.

[00247] 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 URI, 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.

[00248] 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.

[00249] 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.

[00250] 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 requester 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 requestor attempting to register secure domain name “website.scom” must have previously registered the corresponding non-secure domain name “website.com”.

[00251] 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.

[00252] 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.

[00253] 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

[00254] 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.

[00255] 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.

[00256] 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.

[00257] 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.

[00258] 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.

[00259] 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.

[00260] 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.

[00261] 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.

[00262] 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.

[00263] 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.

[00264] 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.

[00265] 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.

[00266] 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.

[00267] 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 for accessing a secure computer network address, comprising steps of:

receiving a secure domain;

sending a query message to a secure domain service, the query message requesting a secure computer network address corresponding to the secure domain;

receiving a response message containing the secure computer network address corresponding to the secure domain; and

sending an access request message to the secure computer network address using a virtual private network communication link.

ABSTRACT

A technique is disclosed for establishing a secure communication link between a first computer and a second computer over a computer network. Initially, a secure communication mode of communication is enabled at a first computer without a user entering any cryptographic information for establishing the secure communication mode of communication. Then, a secure communication link is established between the first computer and a second computer over a computer network based on the enabled secure communication mode of communication. The secure communication link is a virtual private network communication link over the computer network in which one or more data values that vary according to a pseudo-random sequence are inserted into each data packet.

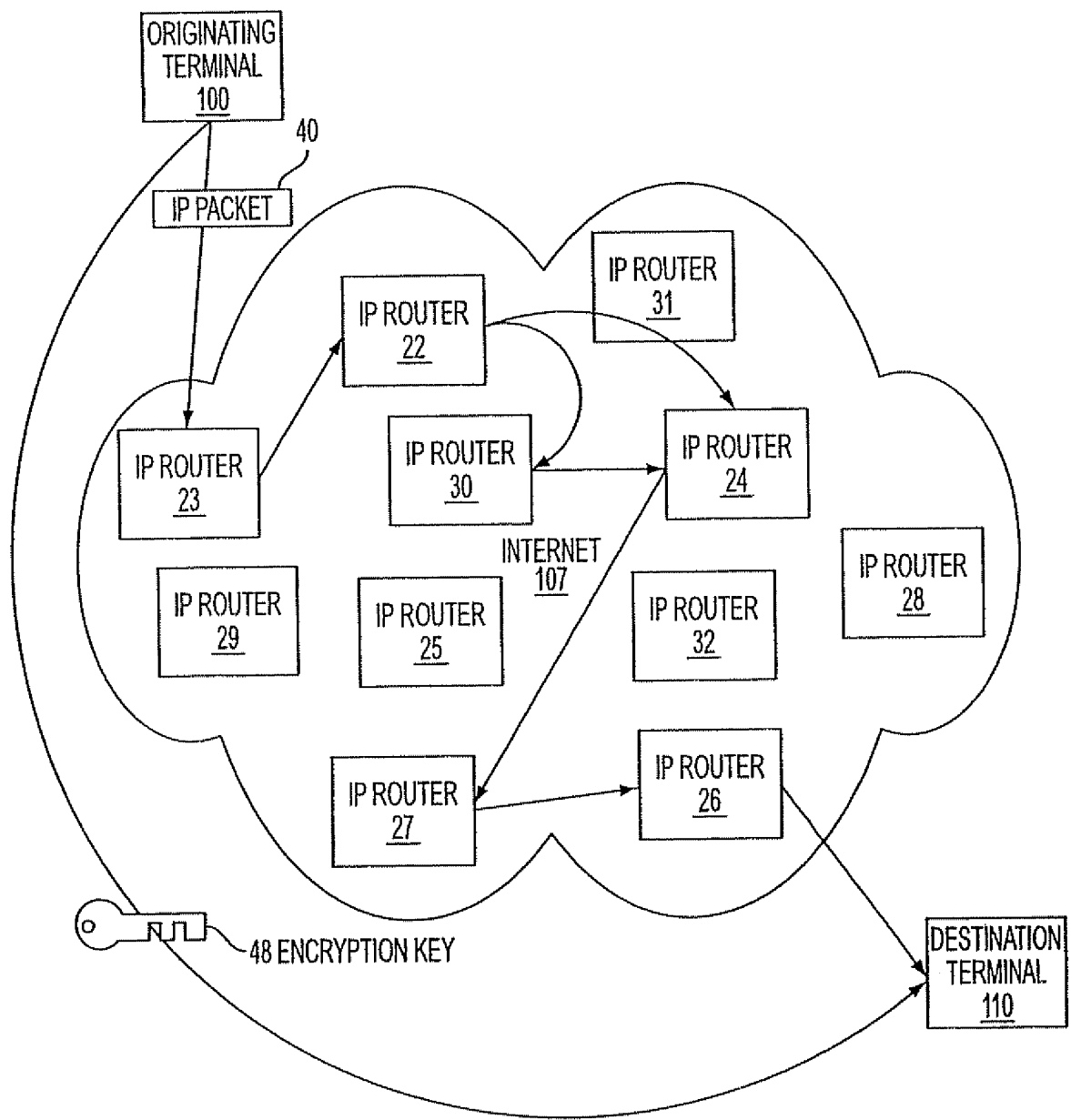


FIG. 1

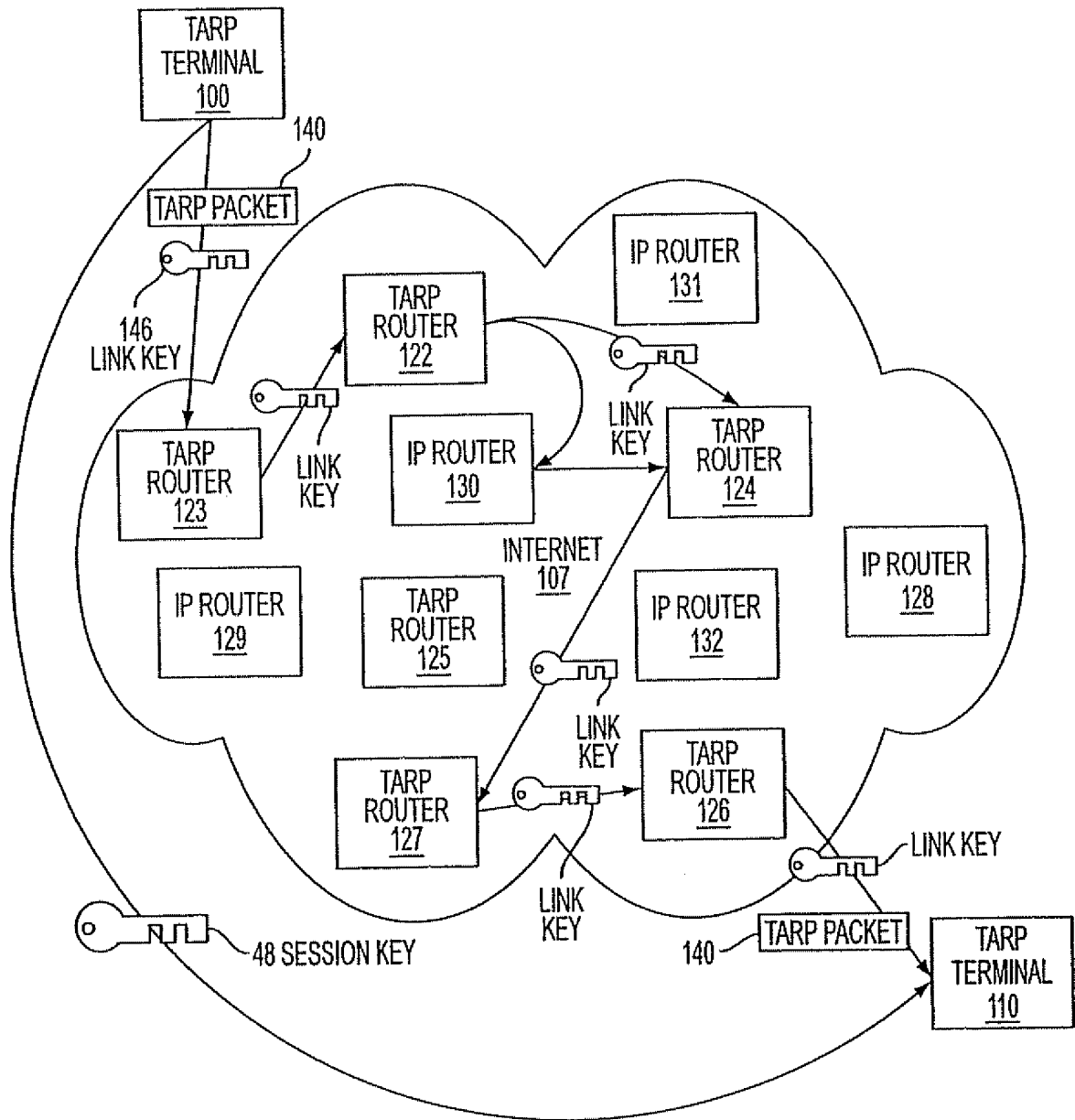


FIG. 2

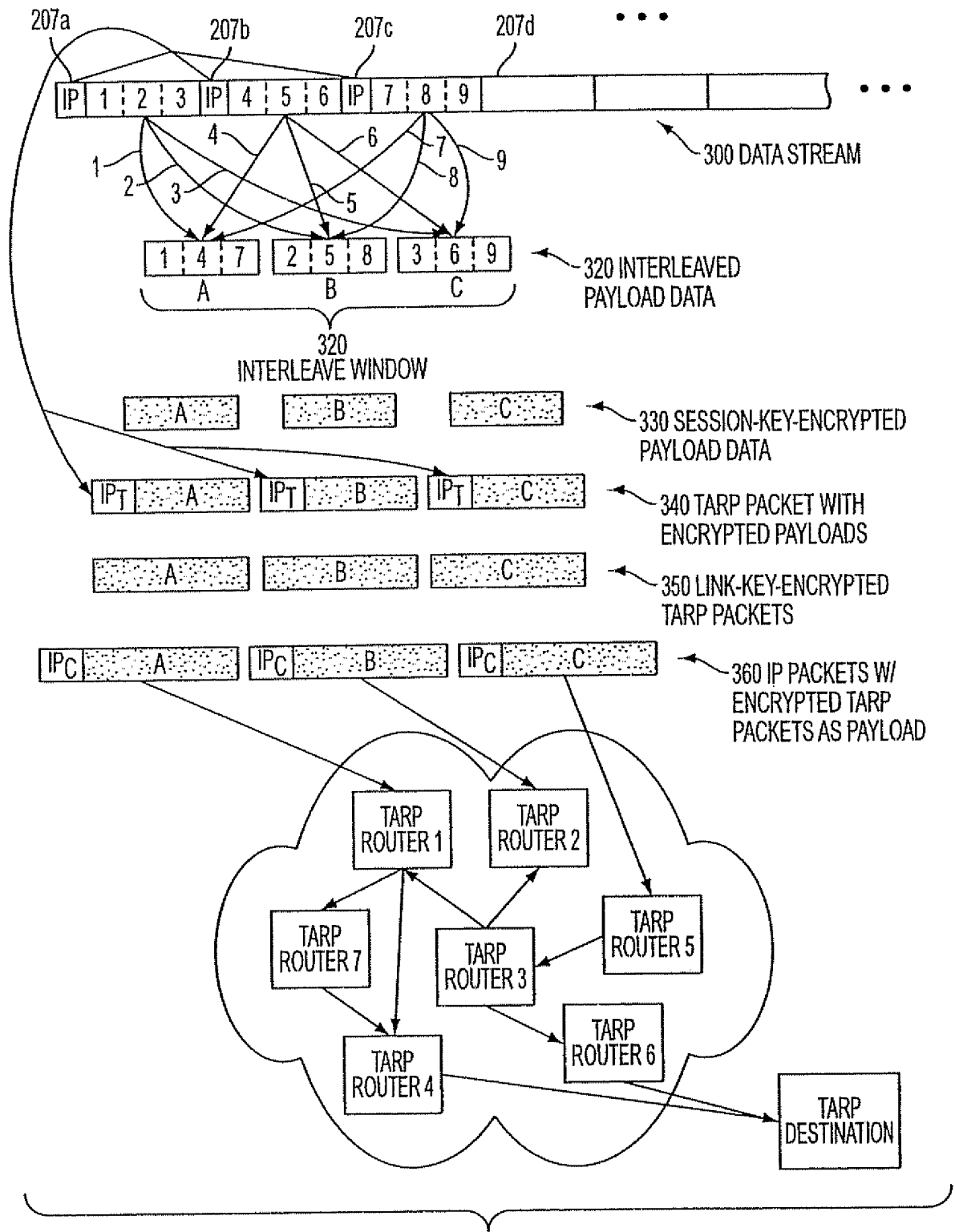


FIG. 3A

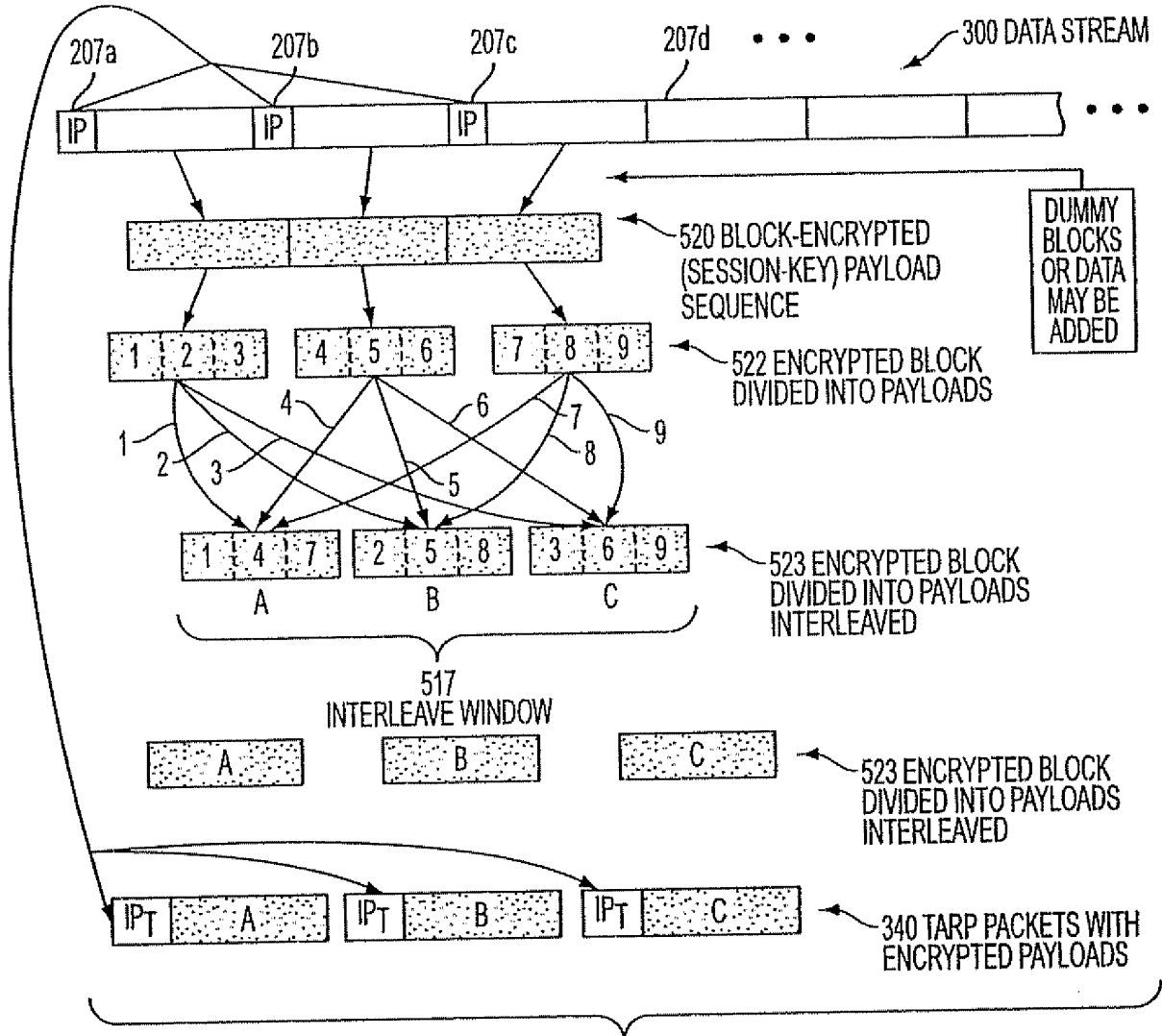


FIG. 3B

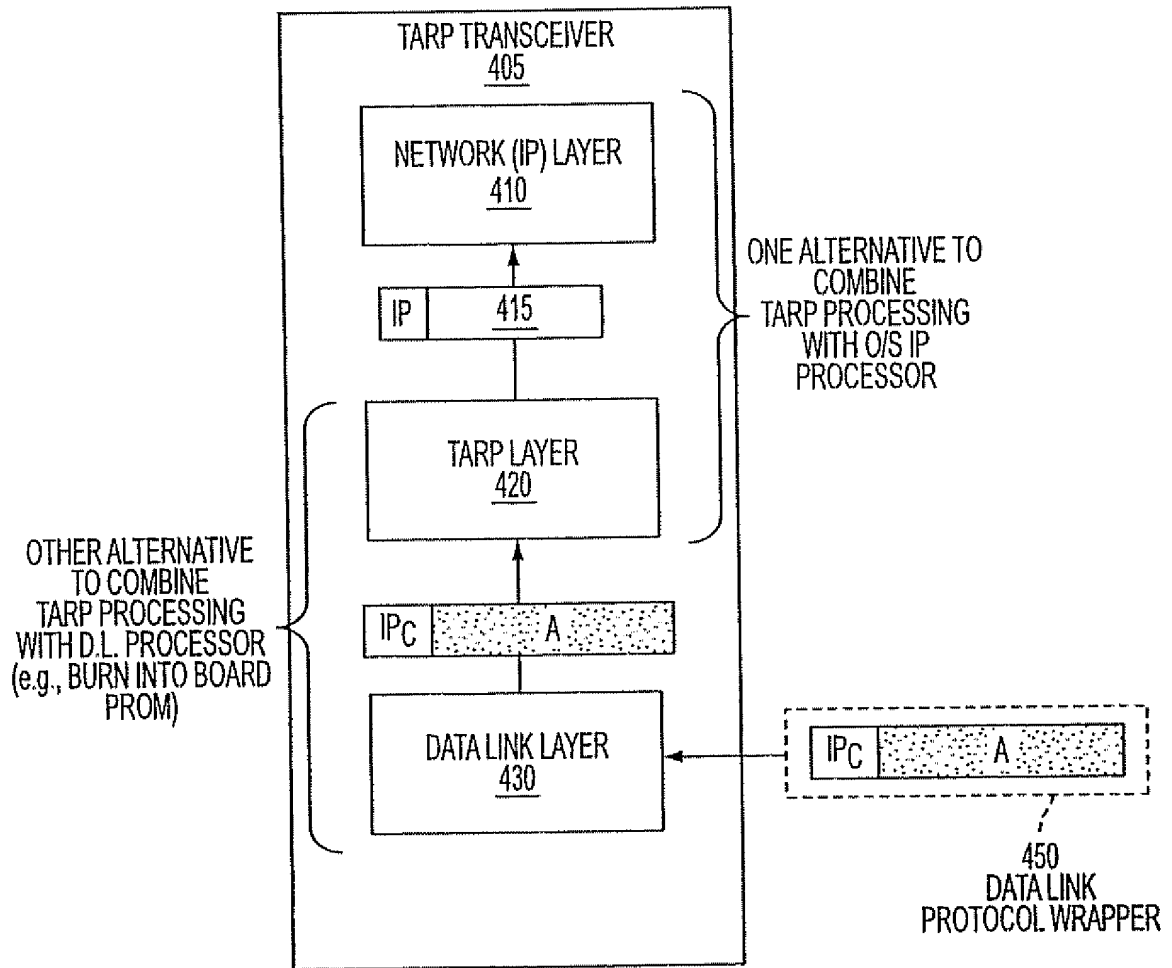


FIG. 4

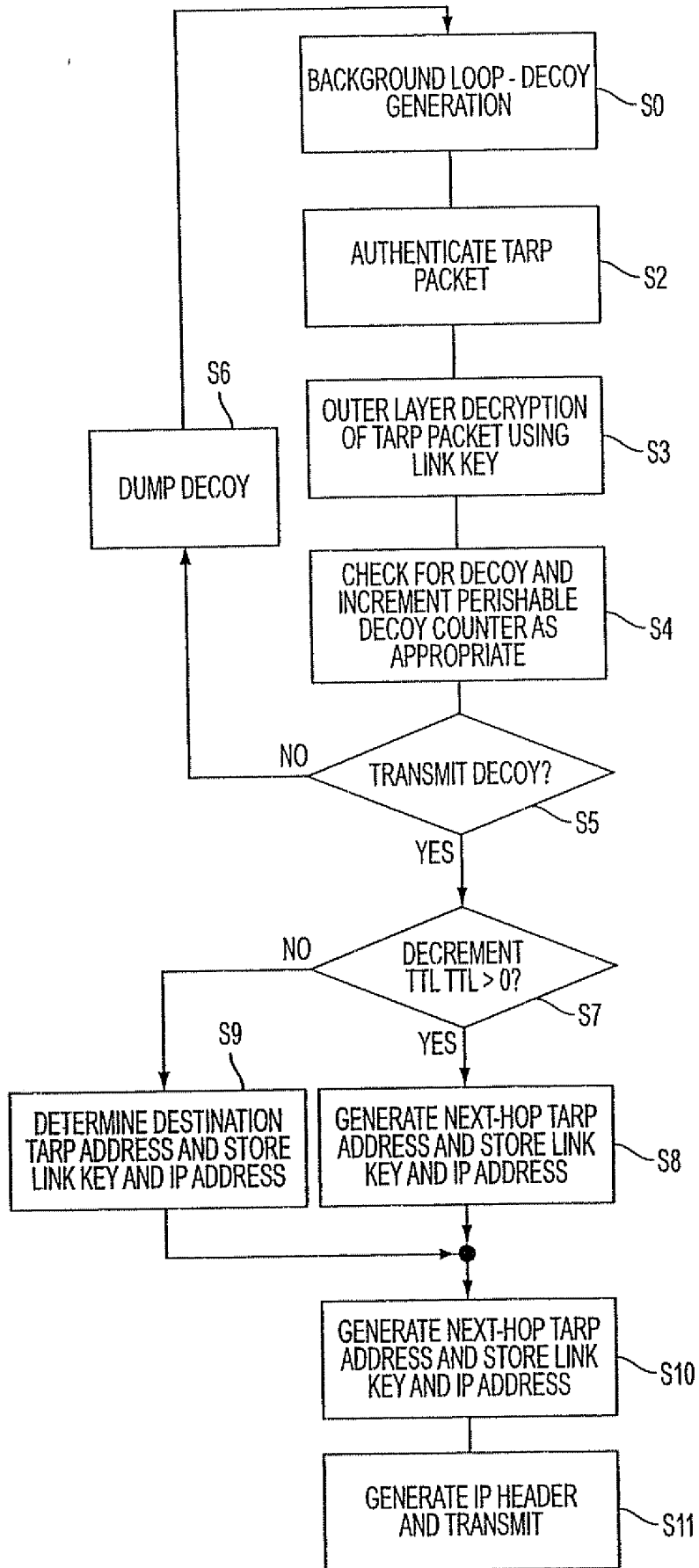


FIG. 5

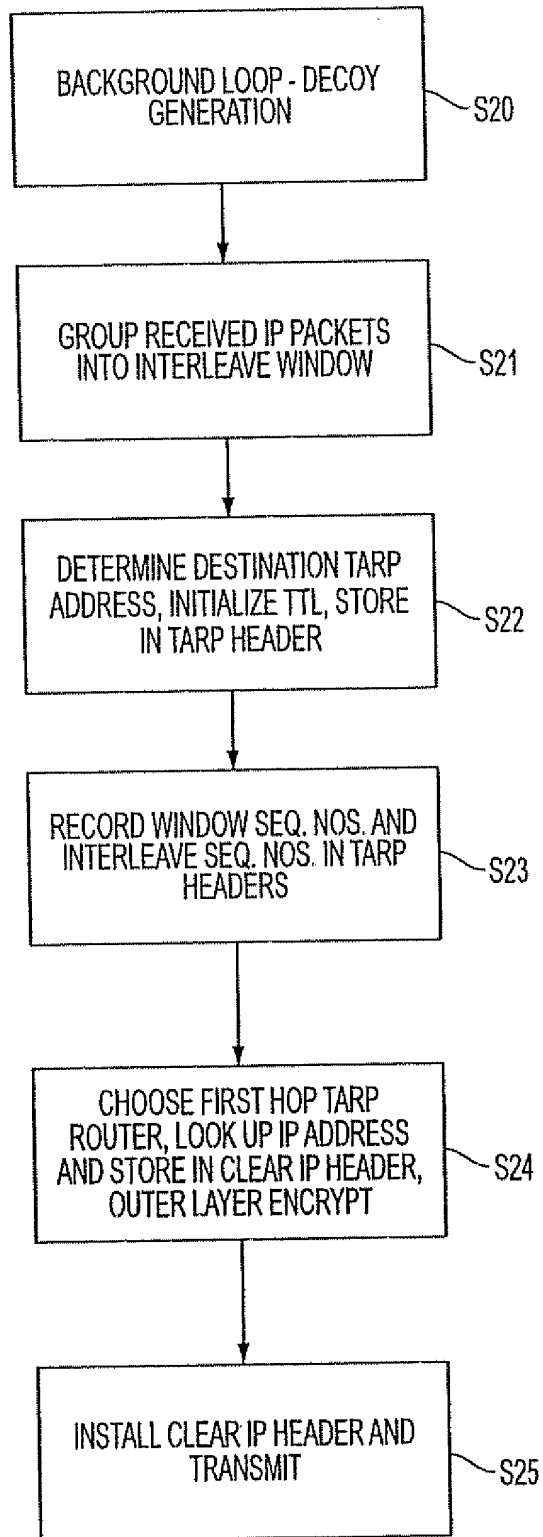


FIG. 6

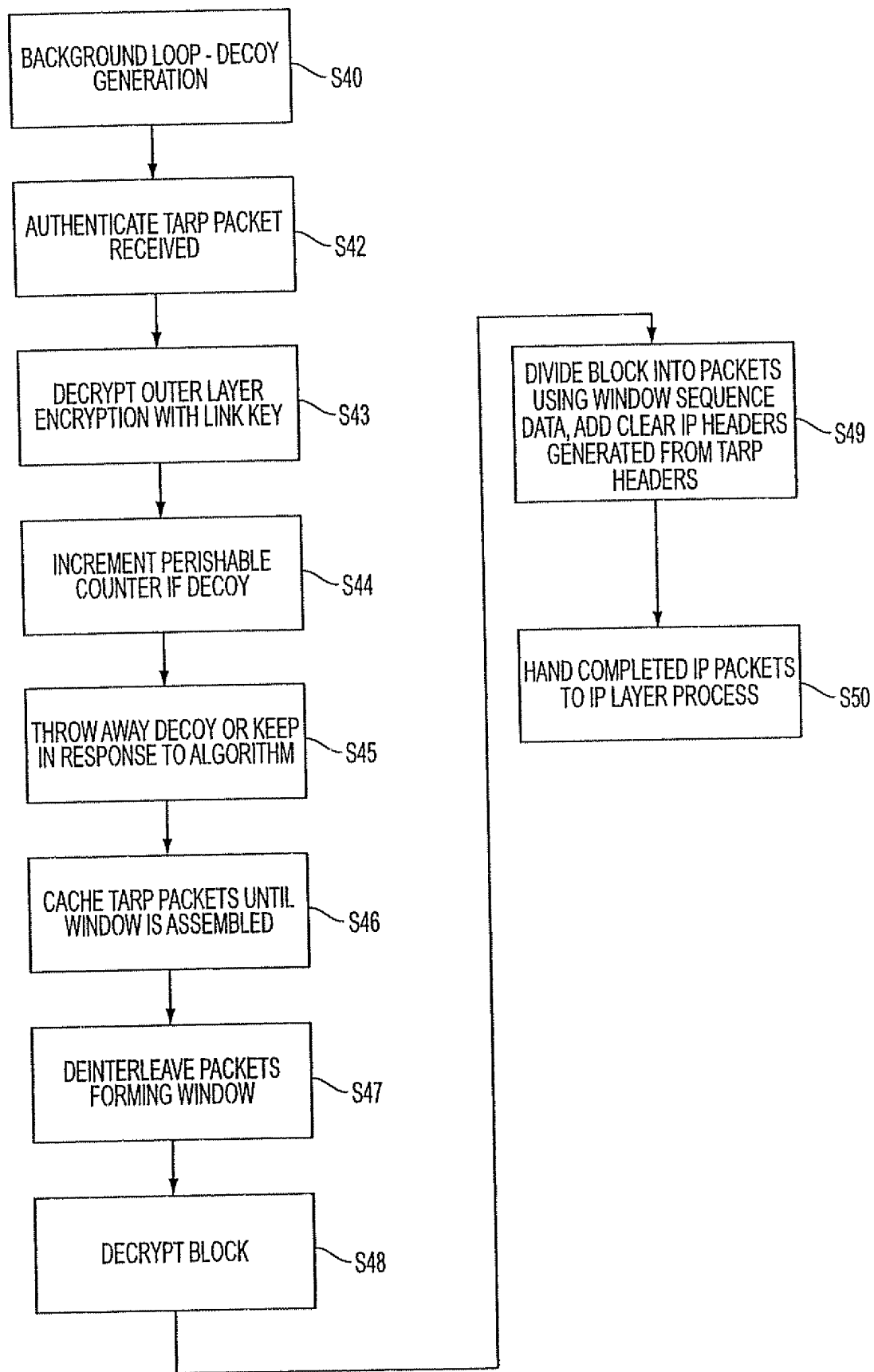


FIG. 7

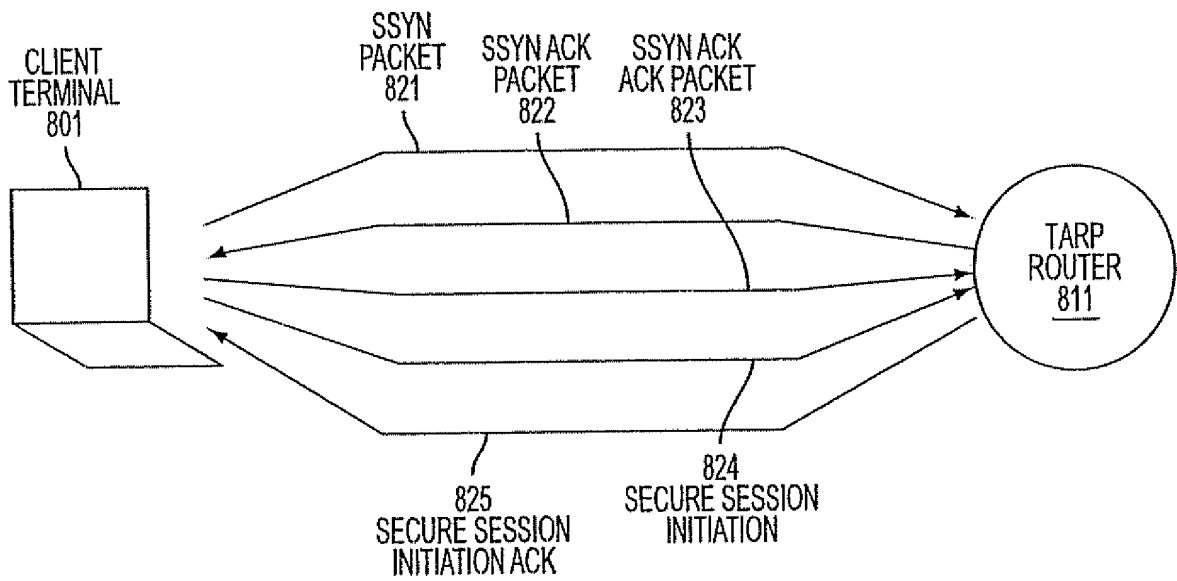
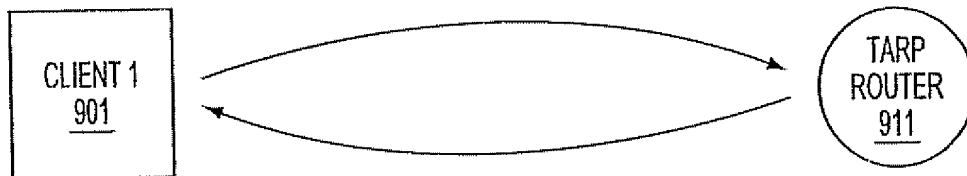


FIG. 8



TRANSMIT TABLE 921		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		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

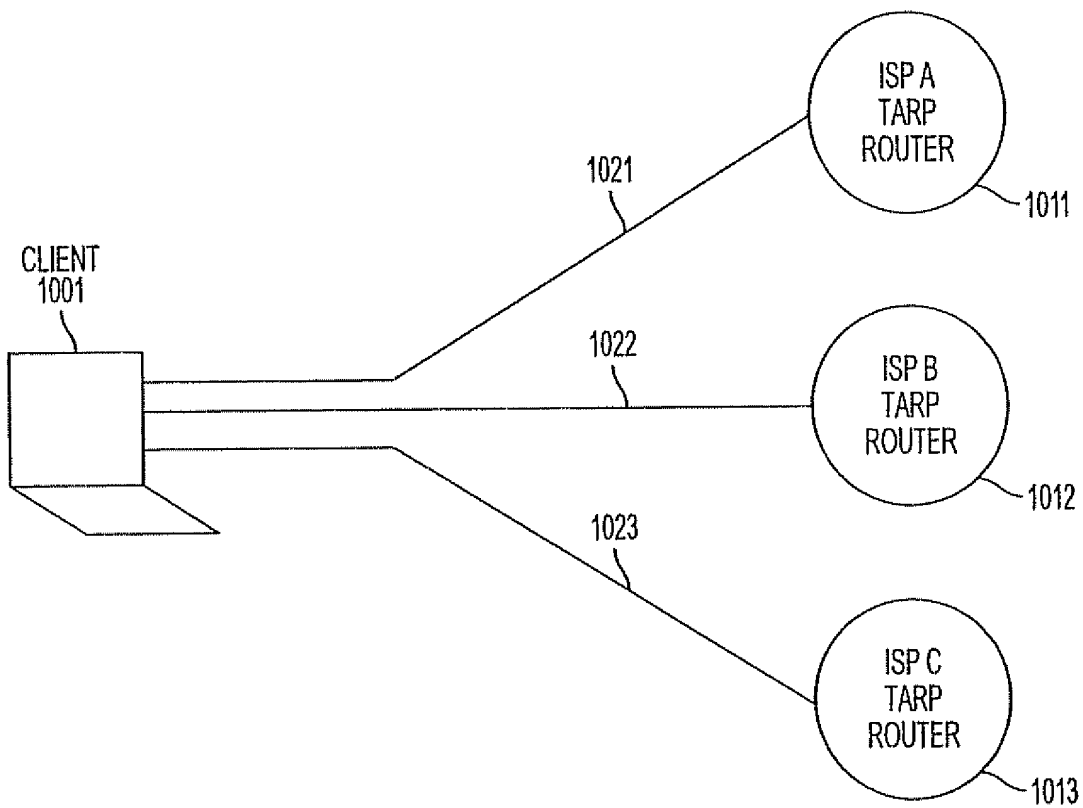


FIG. 10

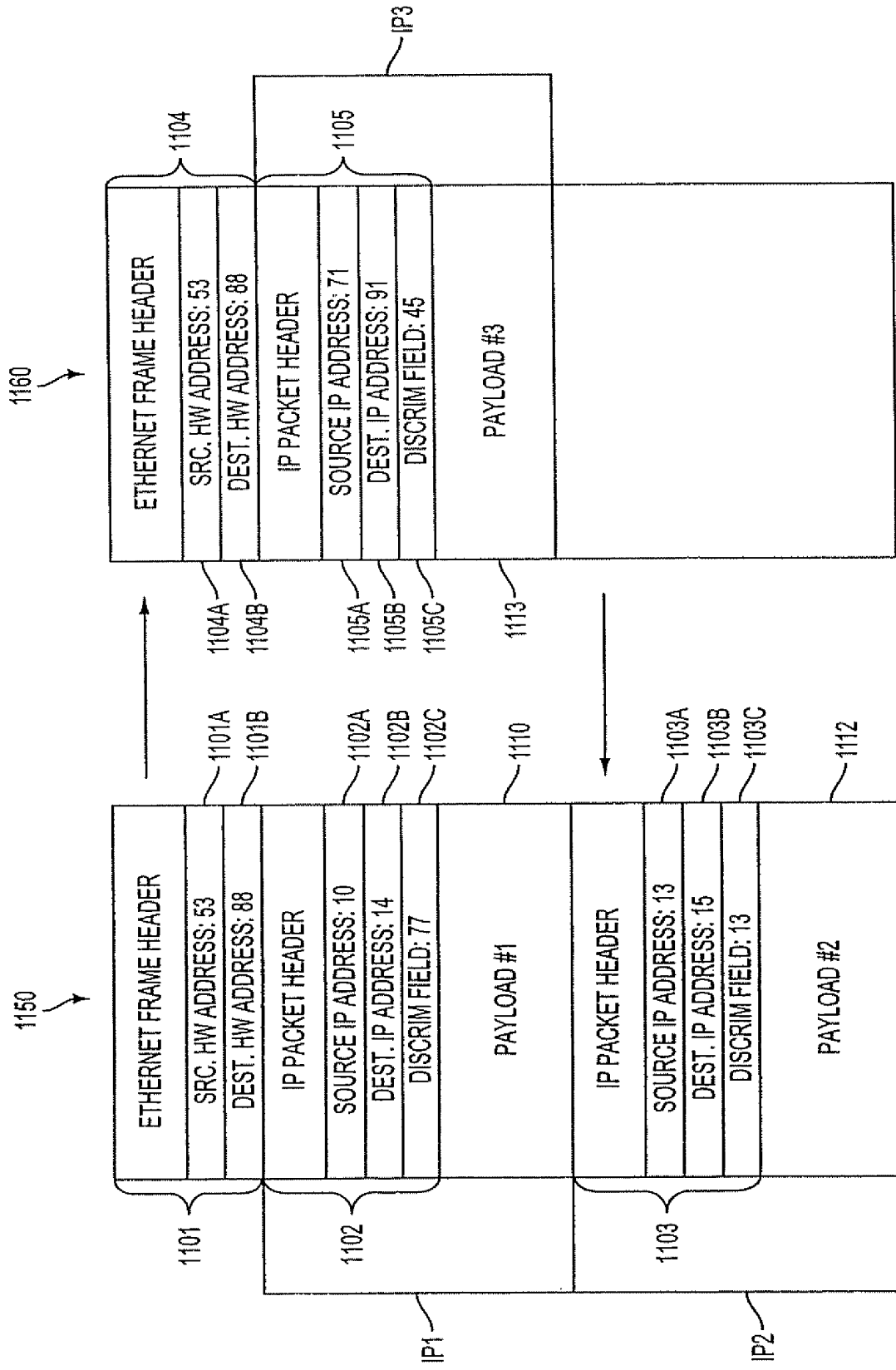


FIG. 11

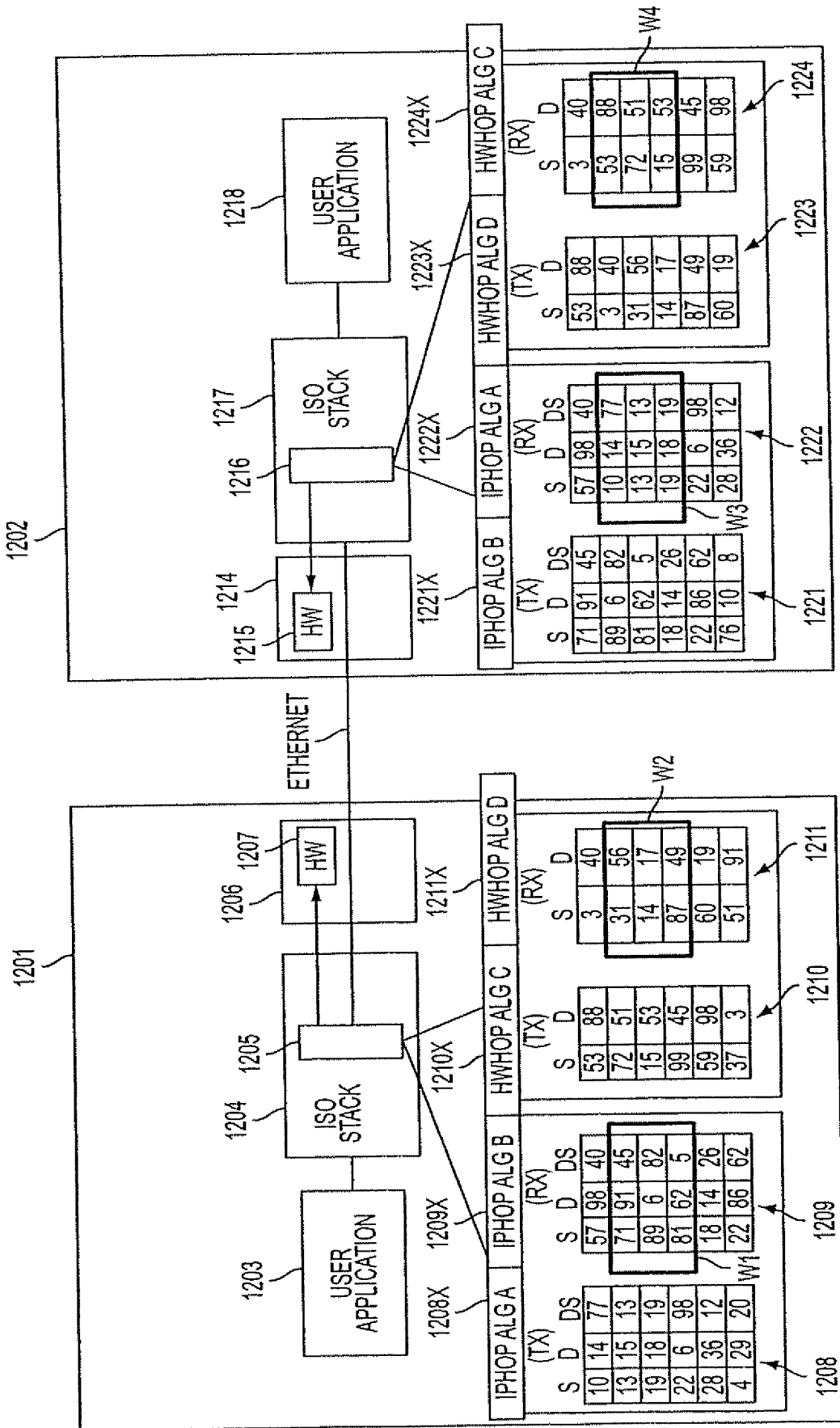


FIG. 12A

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

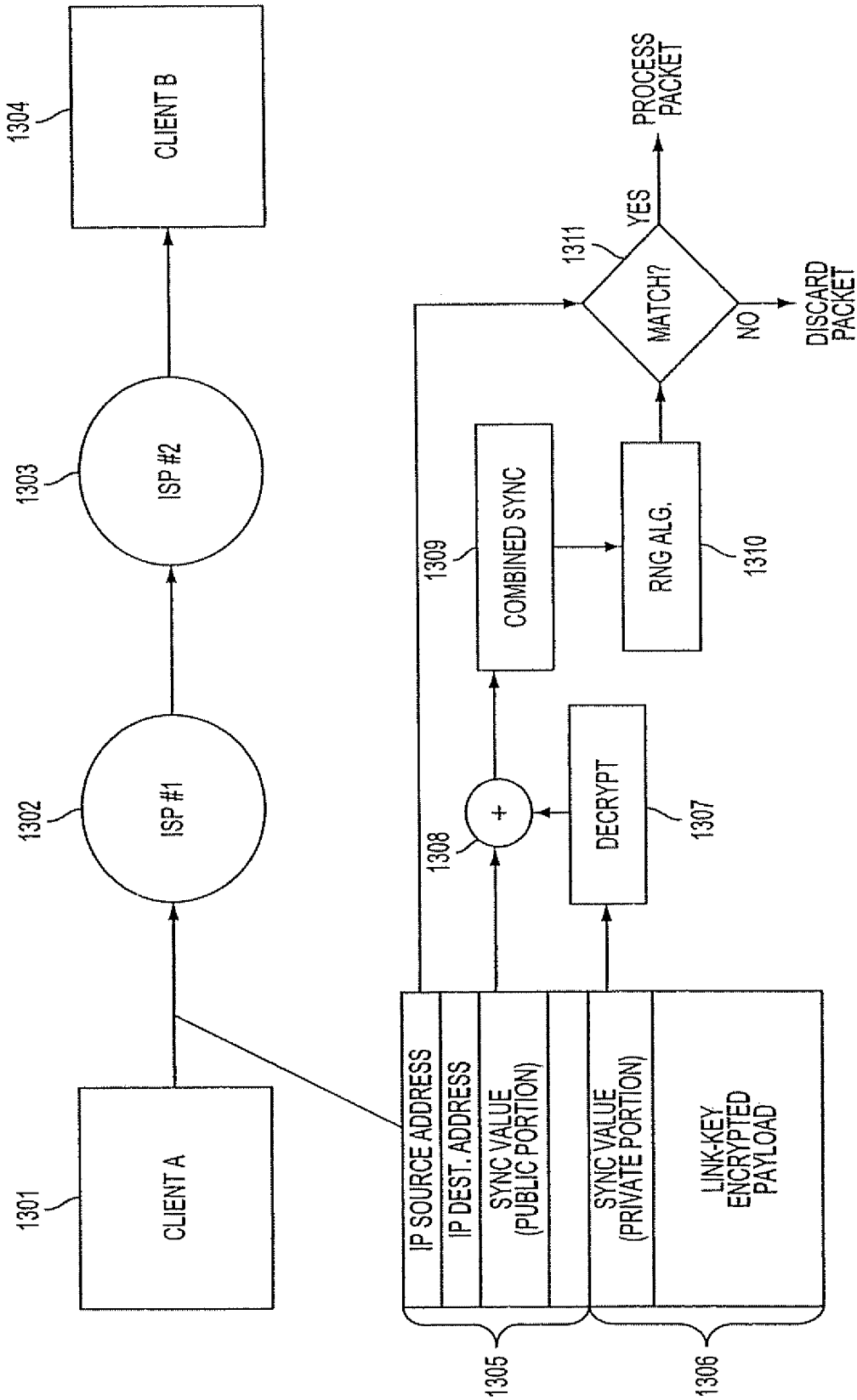


FIG. 13

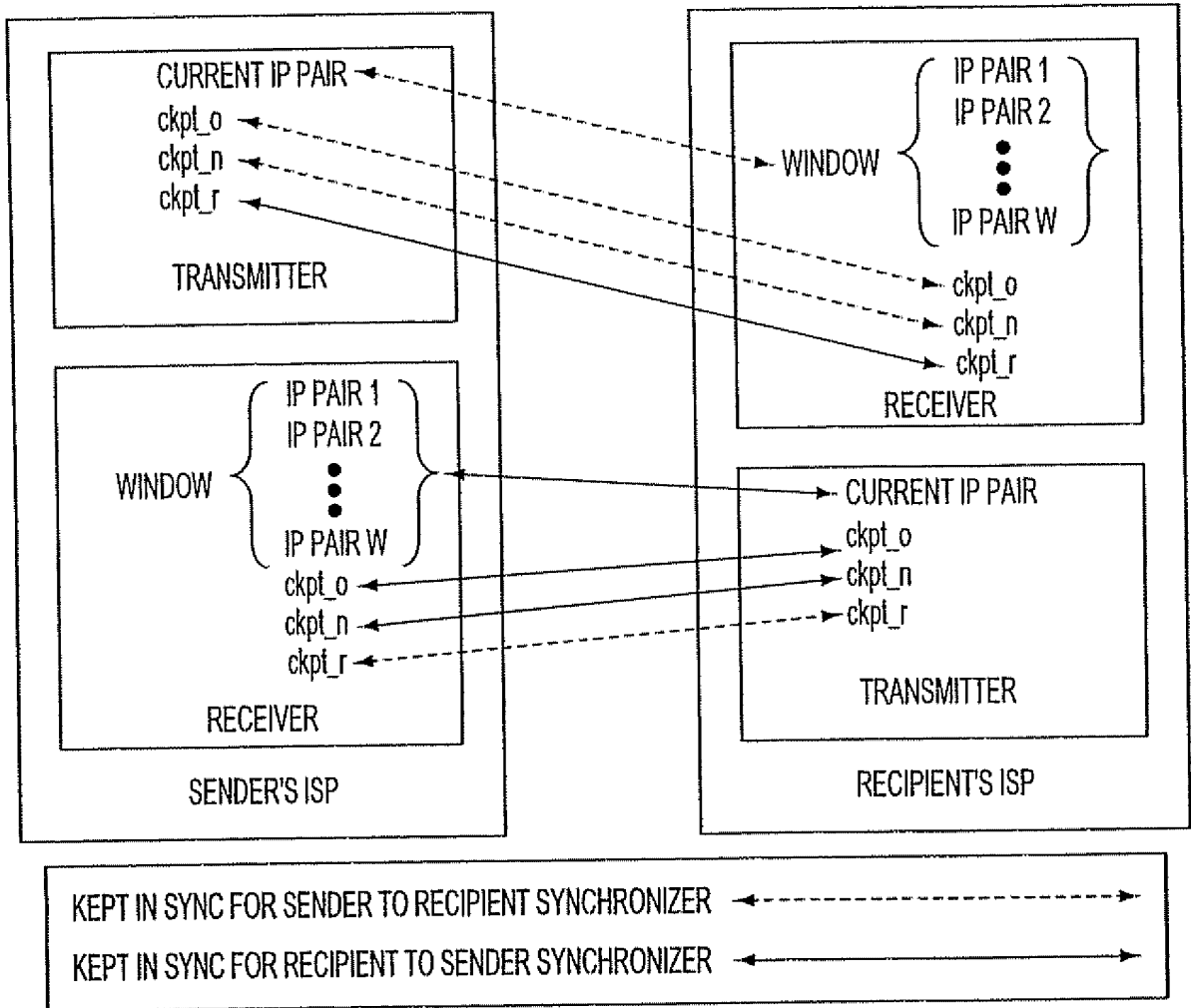


FIG. 14

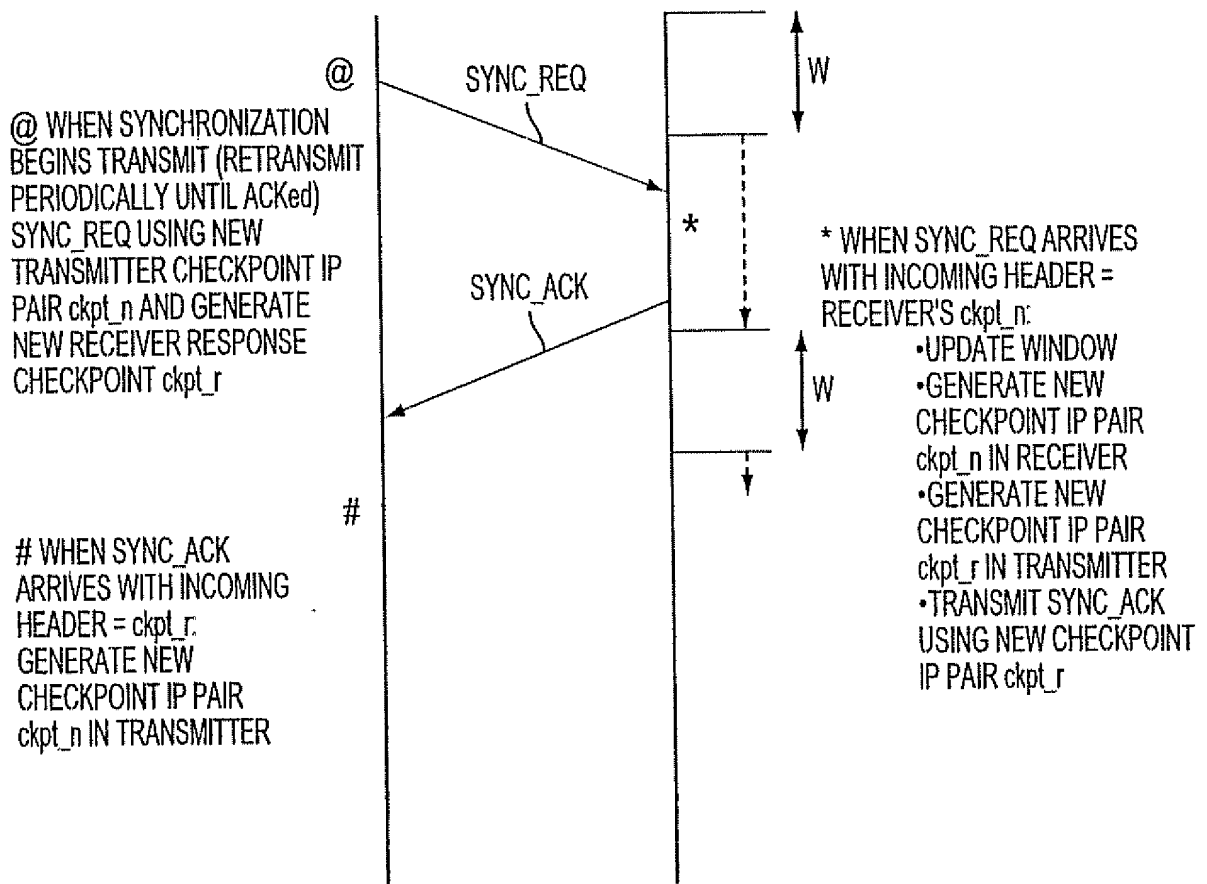


FIG. 15

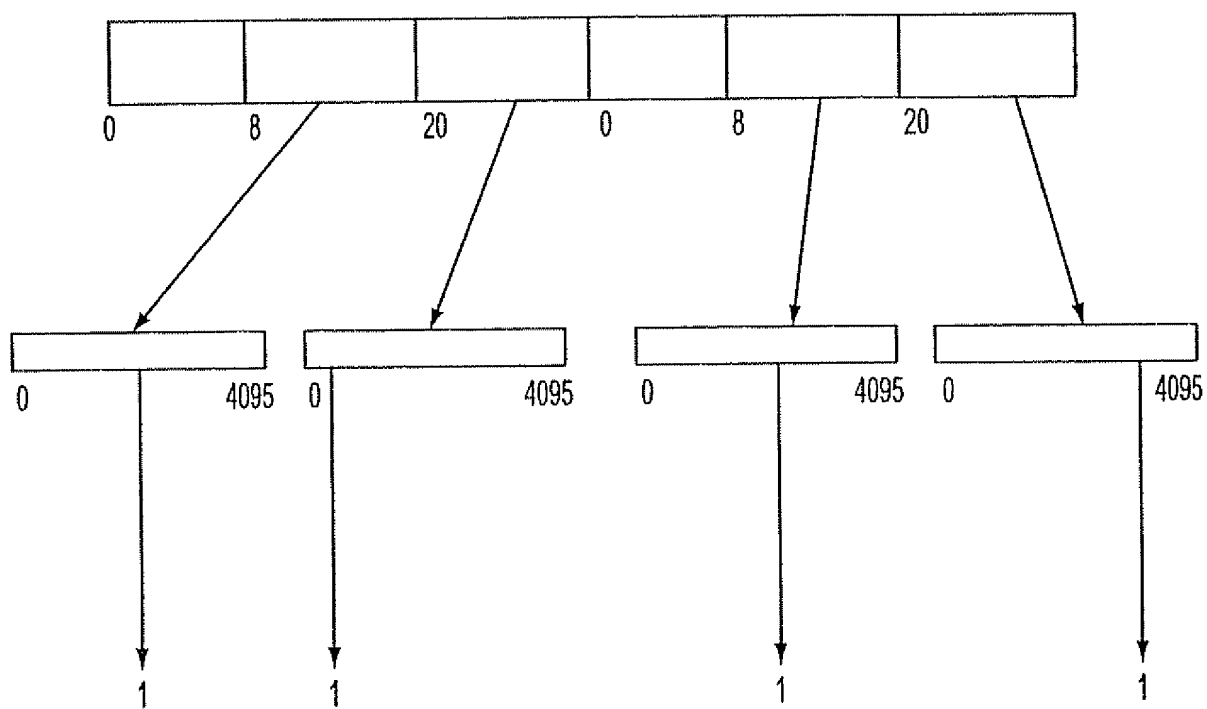


FIG. 16

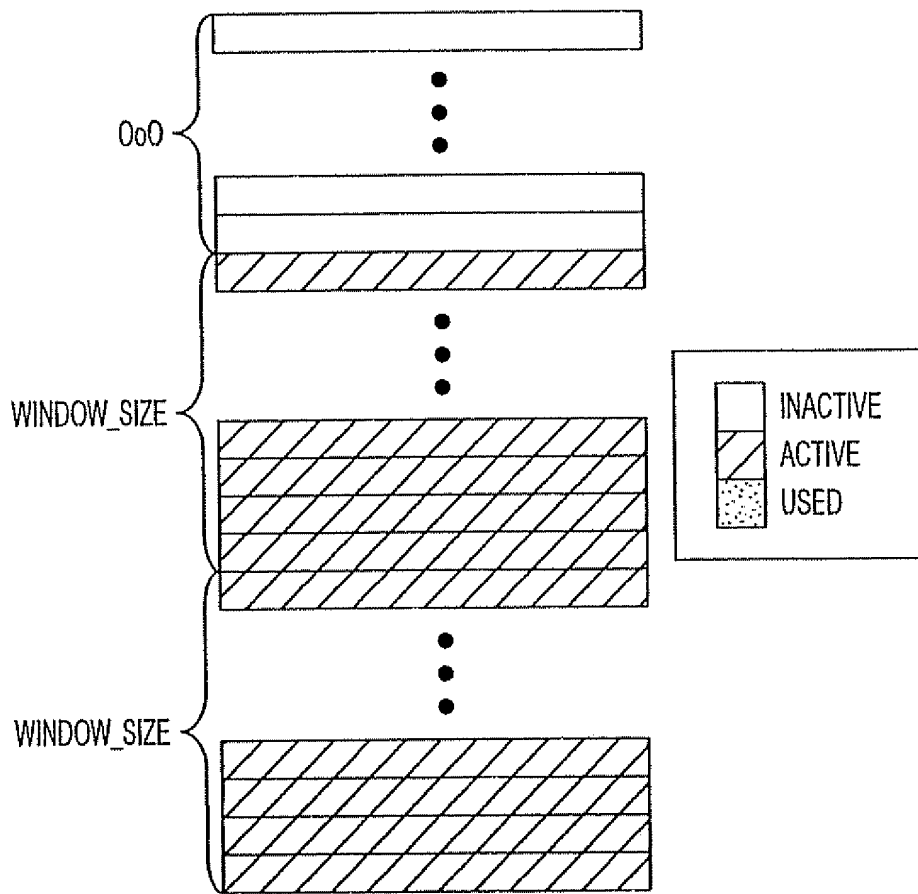


FIG. 17

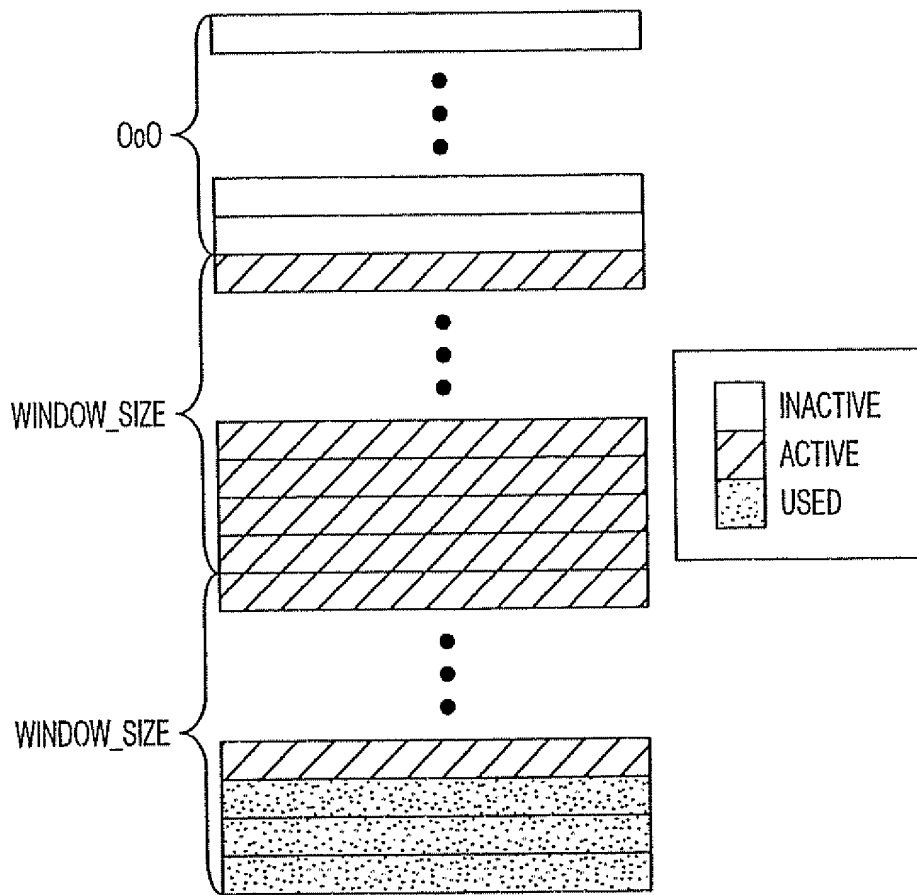


FIG. 18

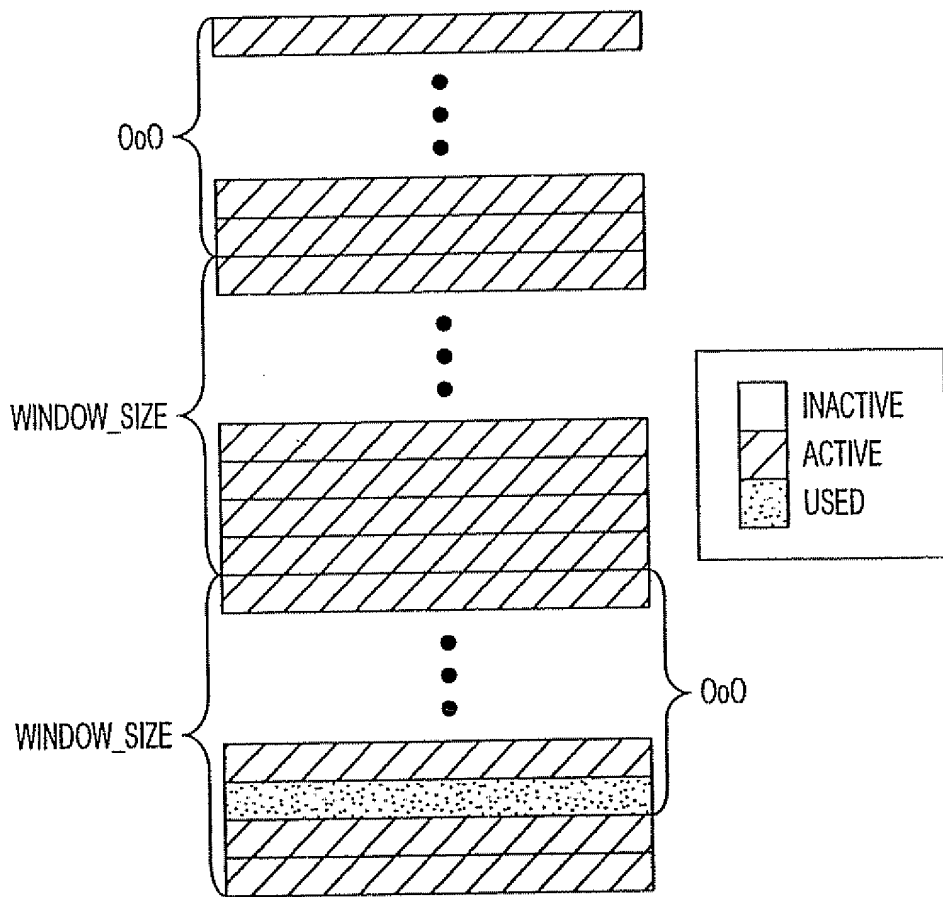


FIG. 19

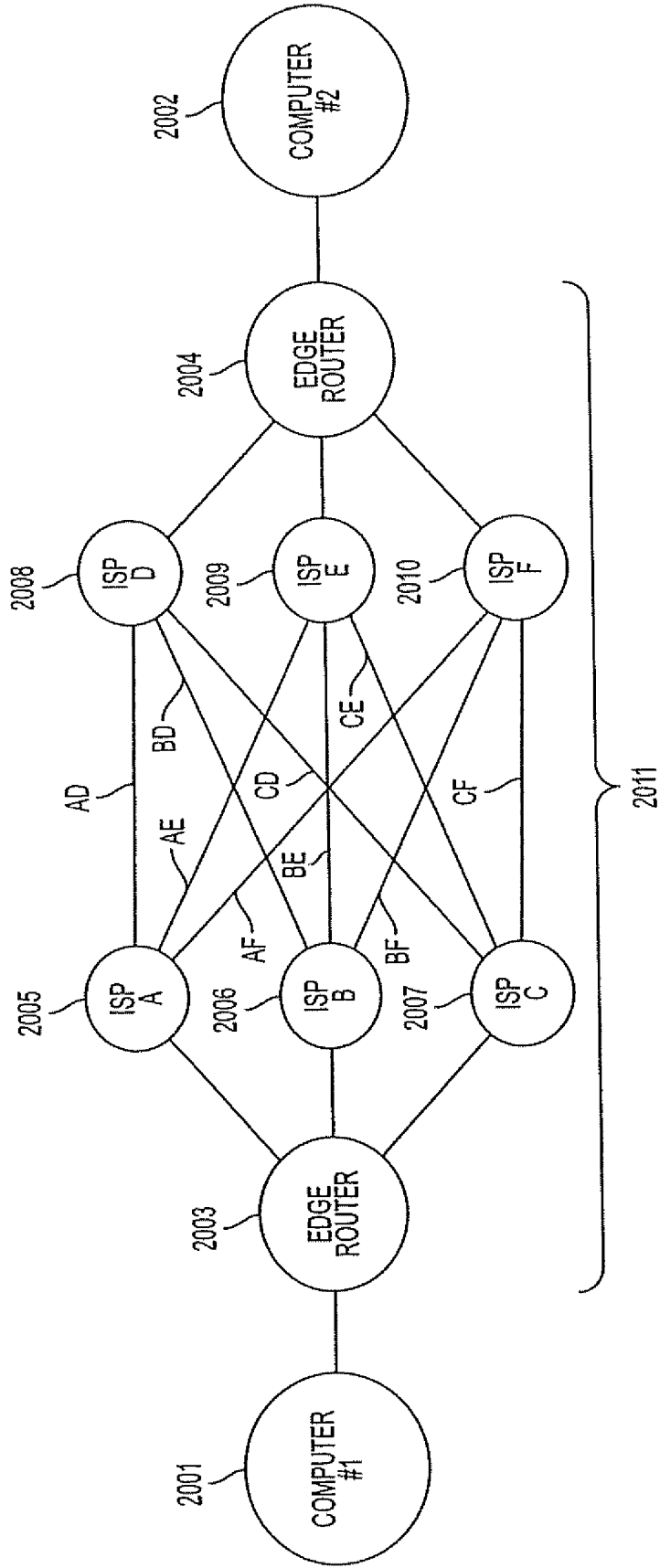


FIG. 20

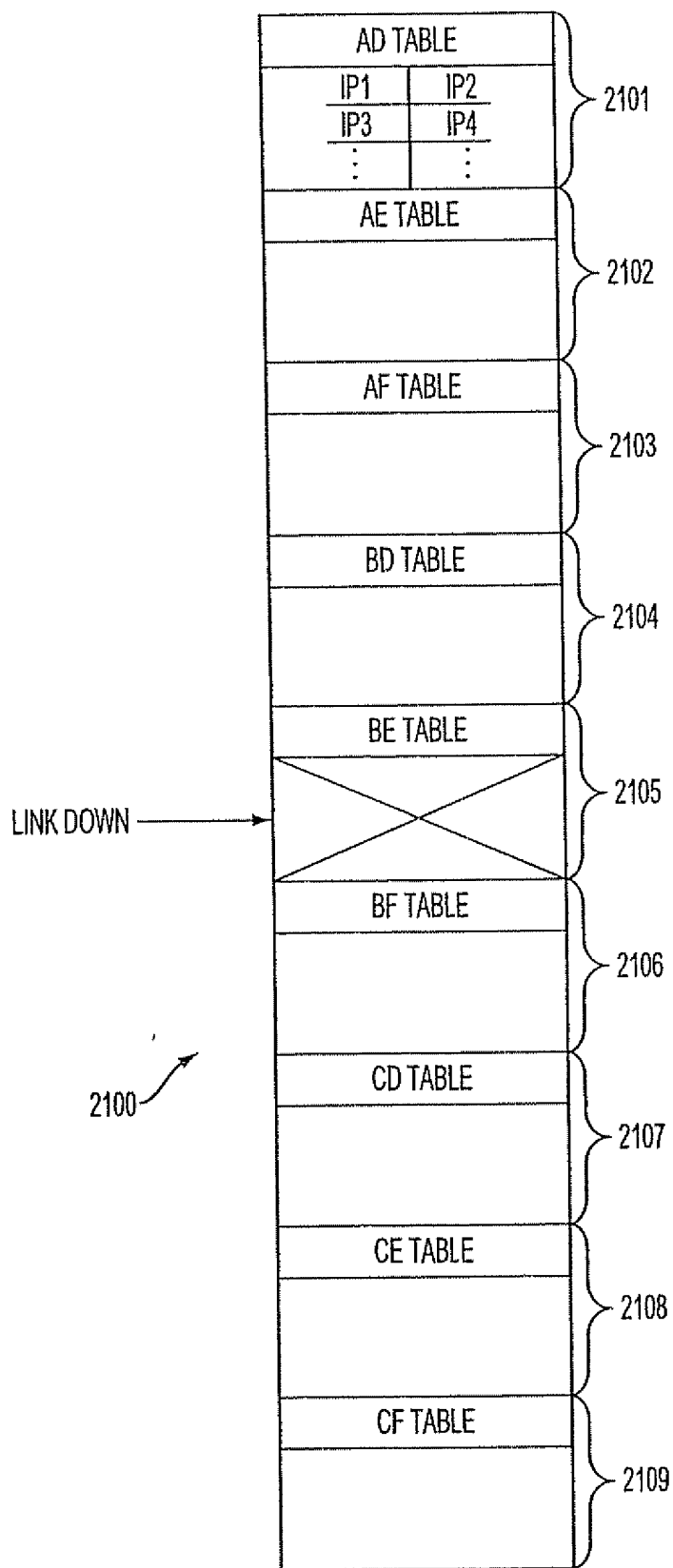


FIG. 21

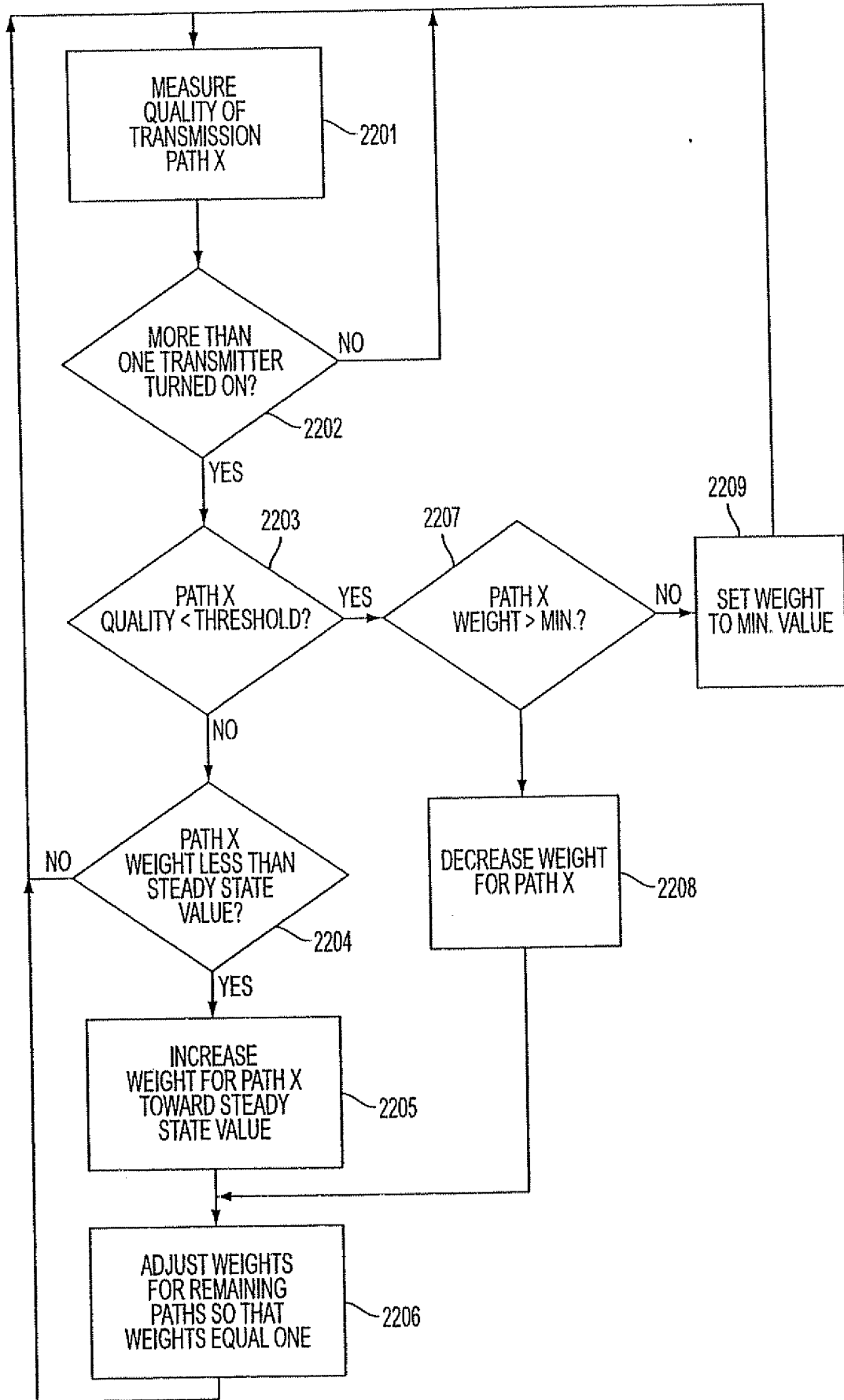


FIG. 22A

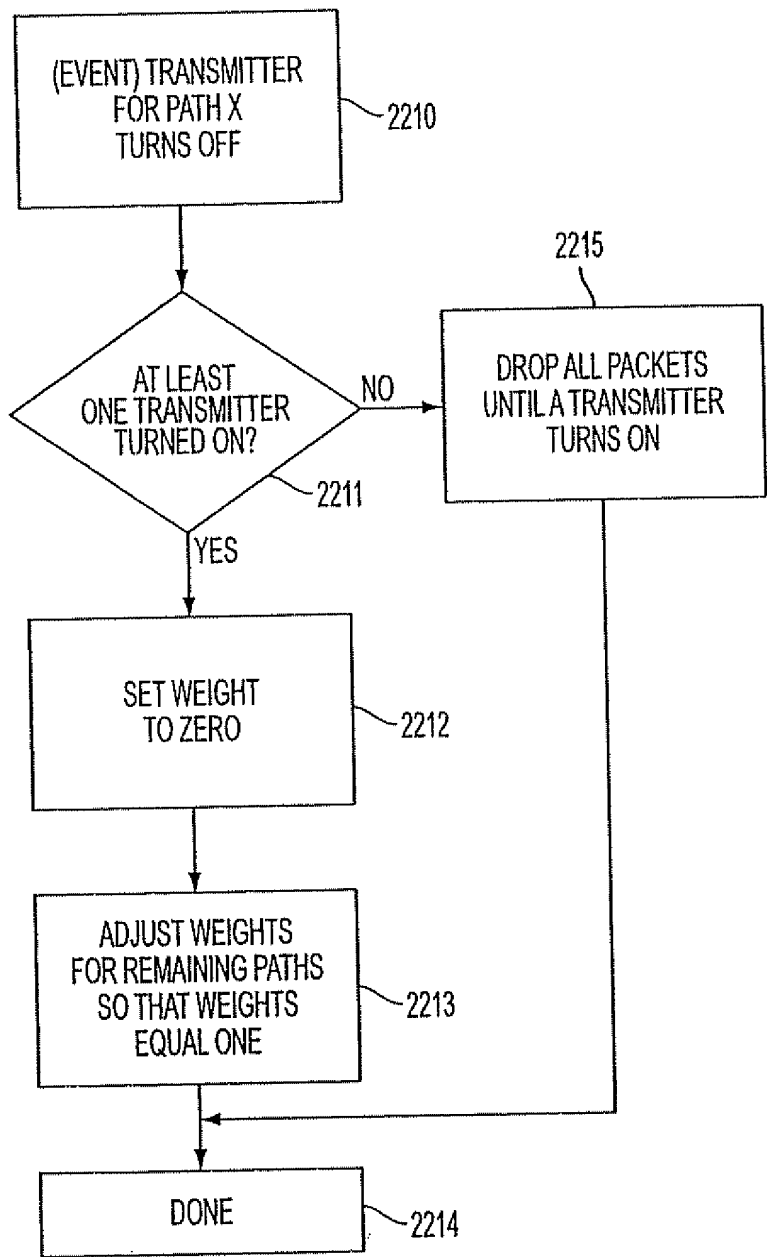


FIG. 22B

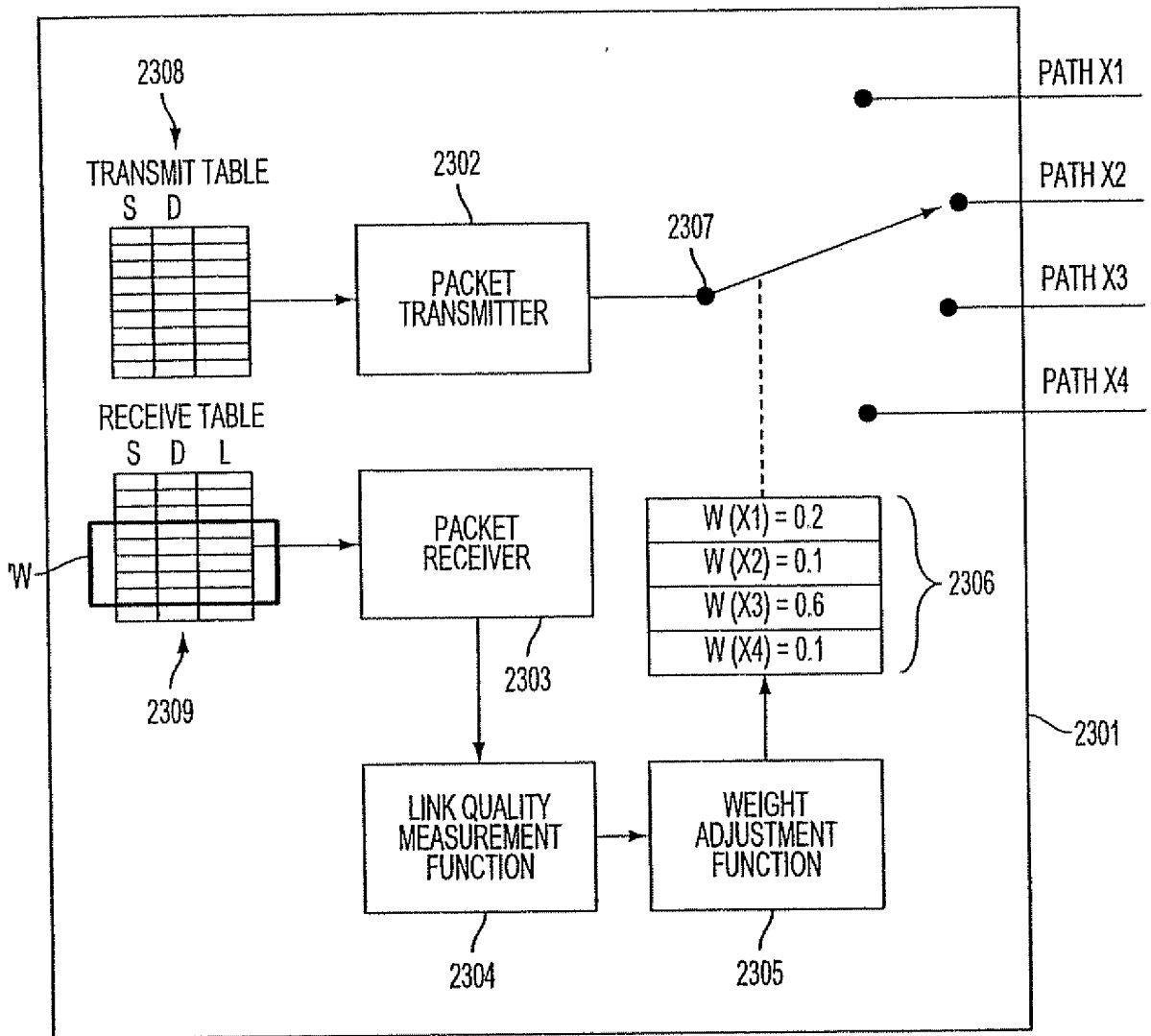


FIG. 23

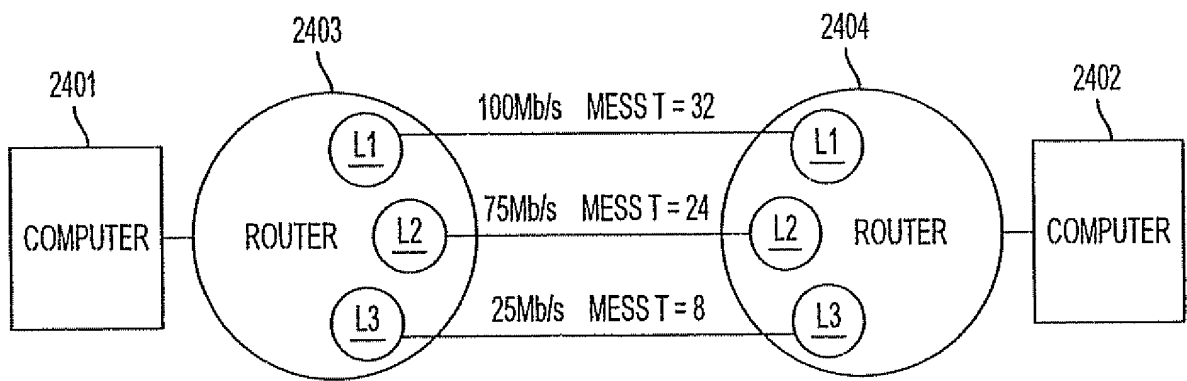


FIG. 24

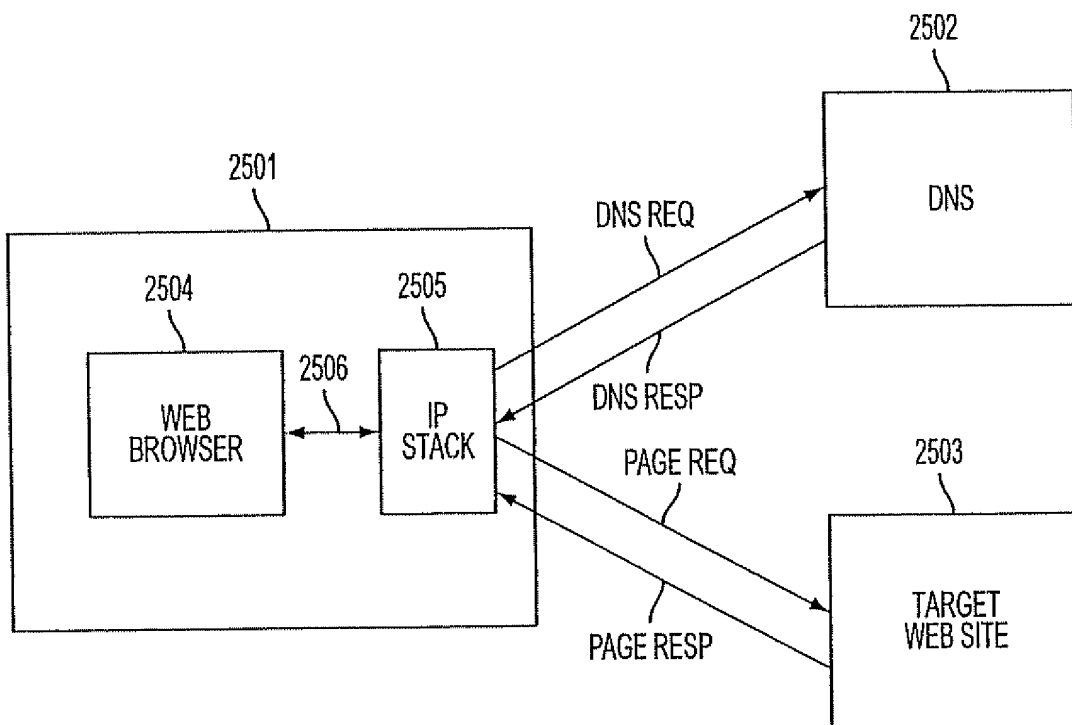


FIG. 25
(PRIOR ART)

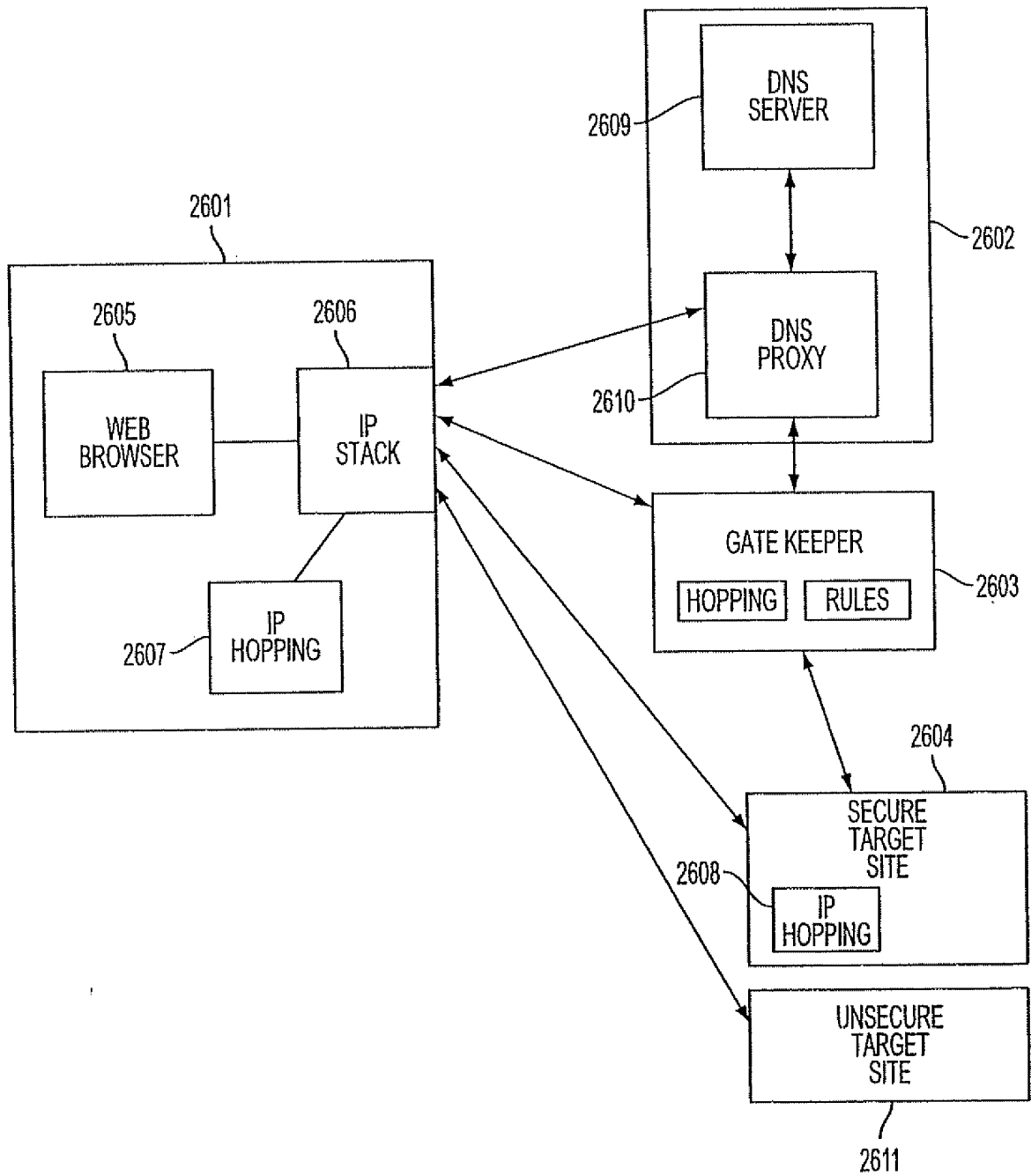


FIG. 26

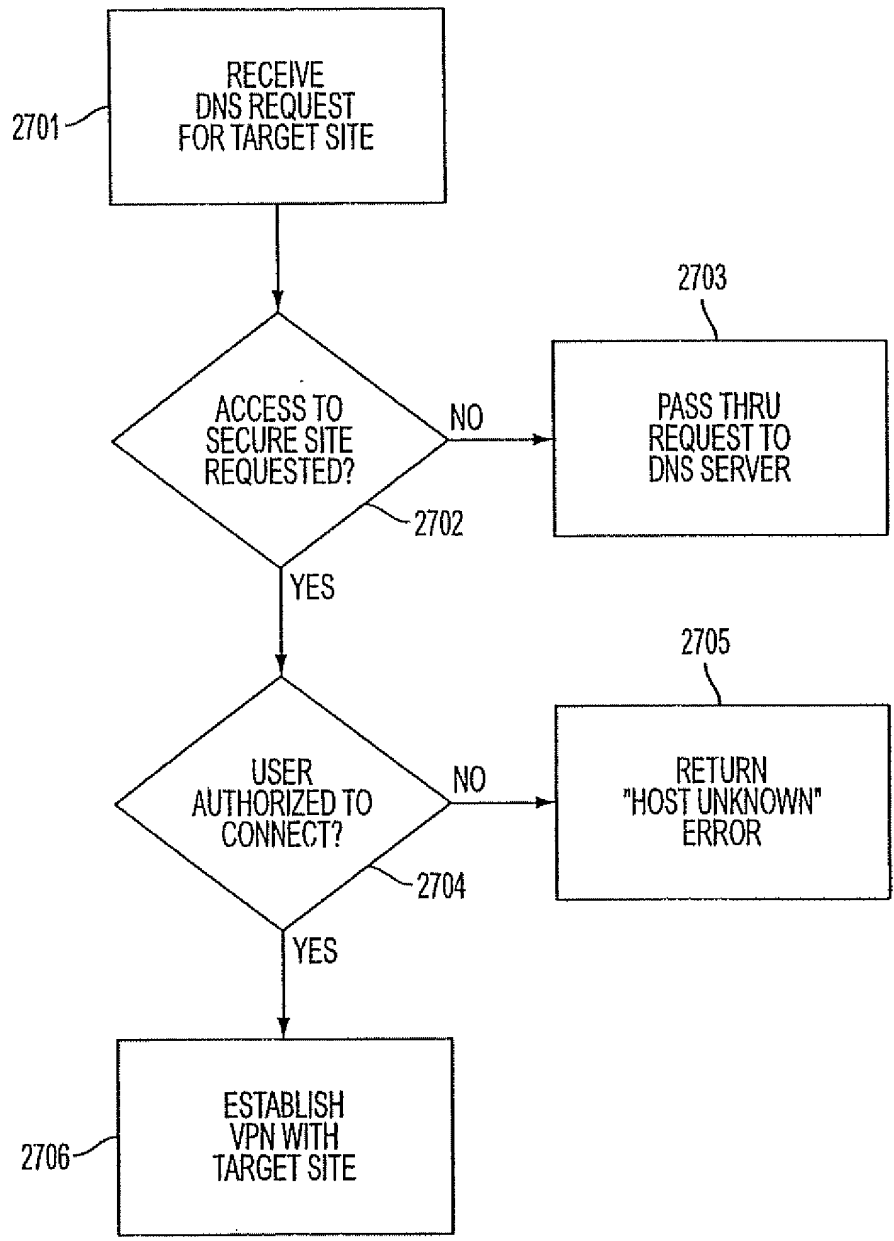


FIG. 27

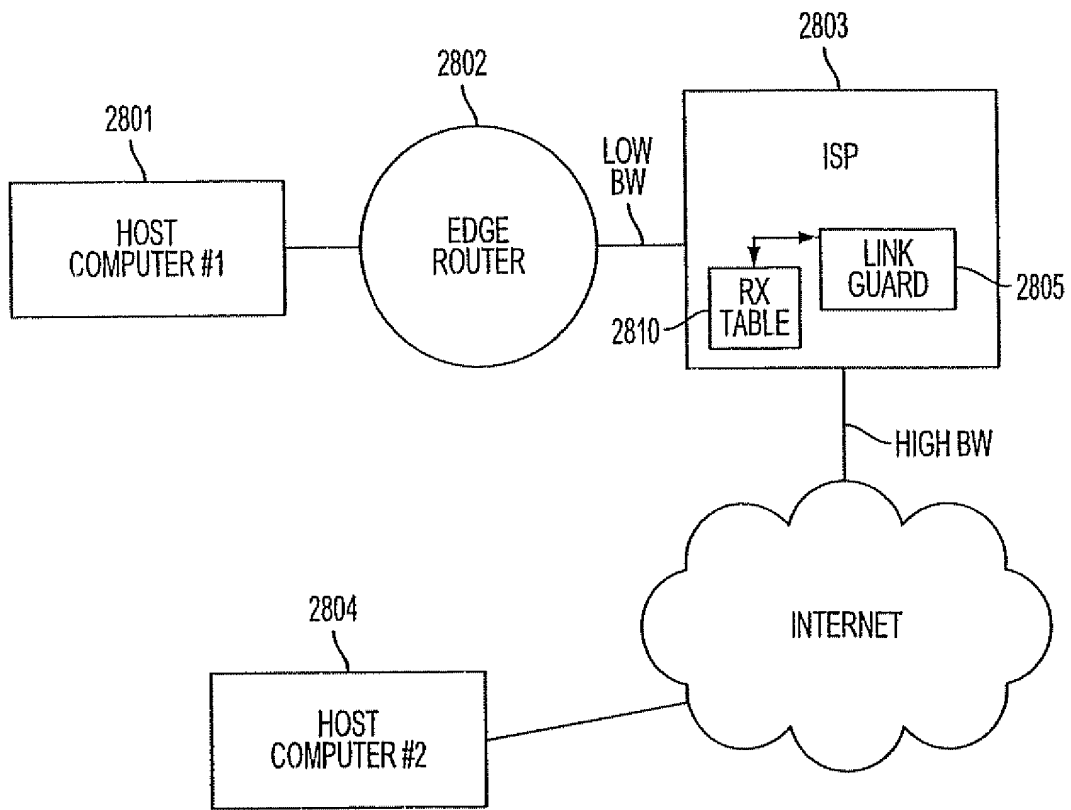


FIG. 28

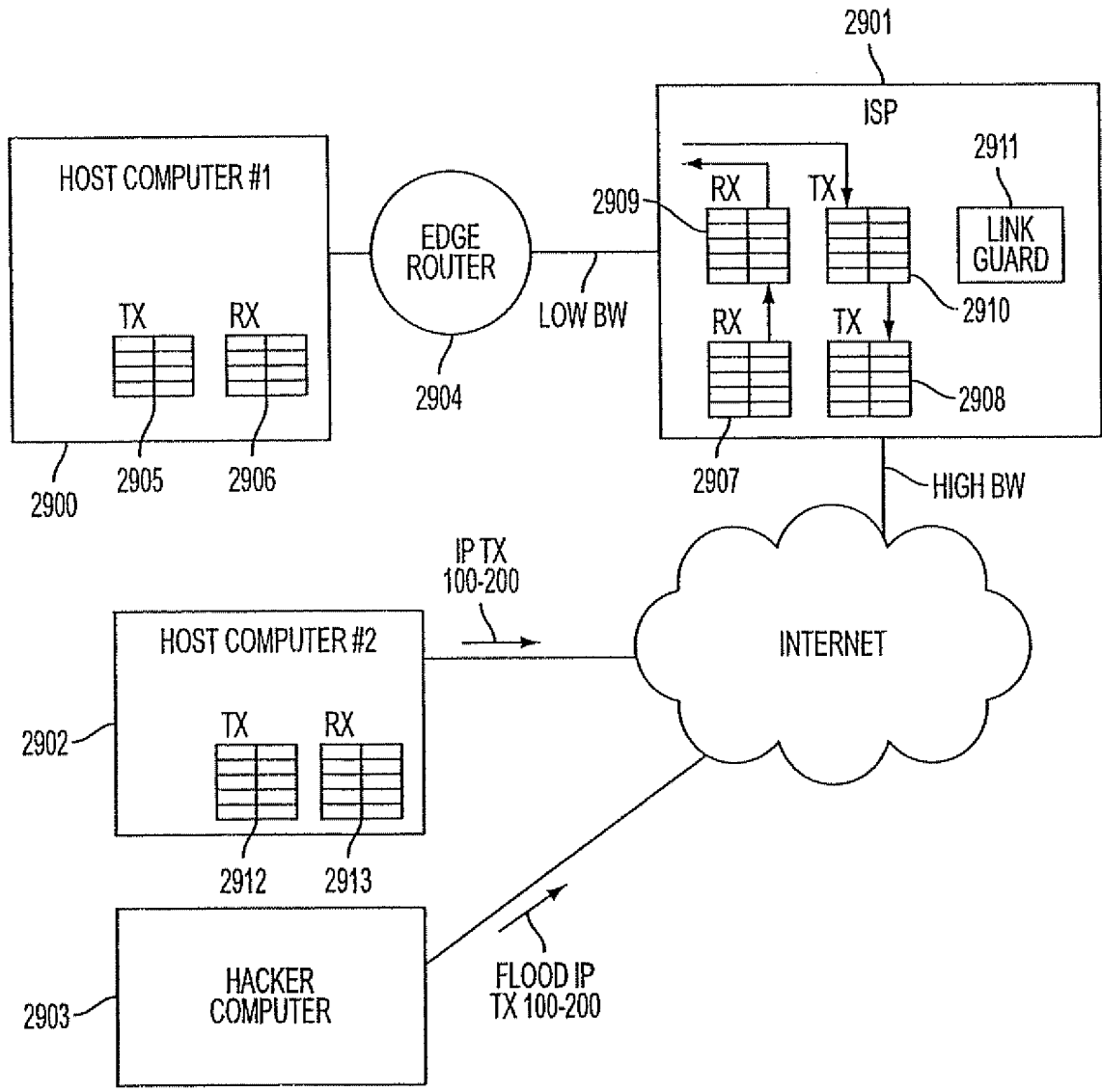


FIG. 29

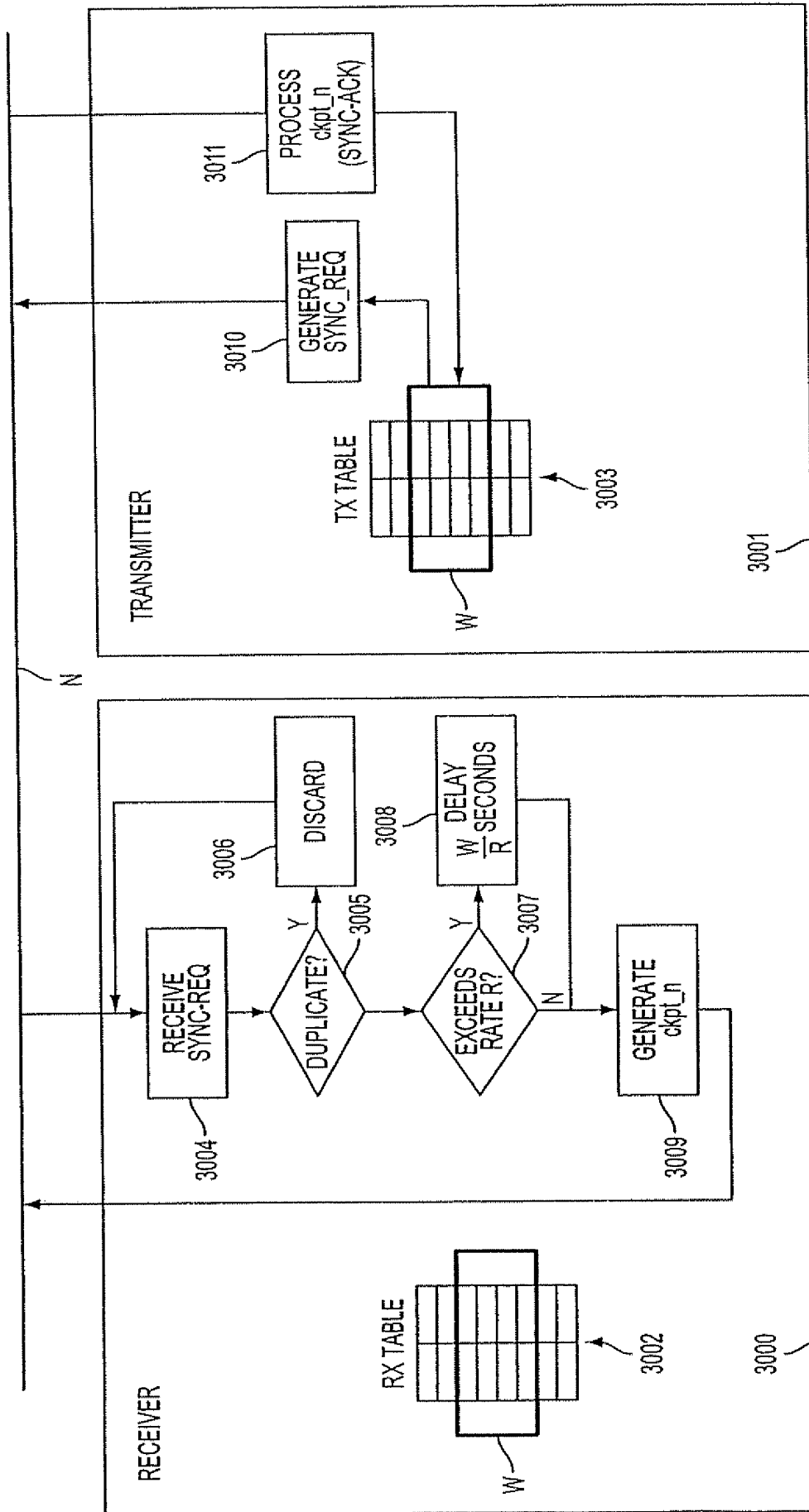


FIG. 30

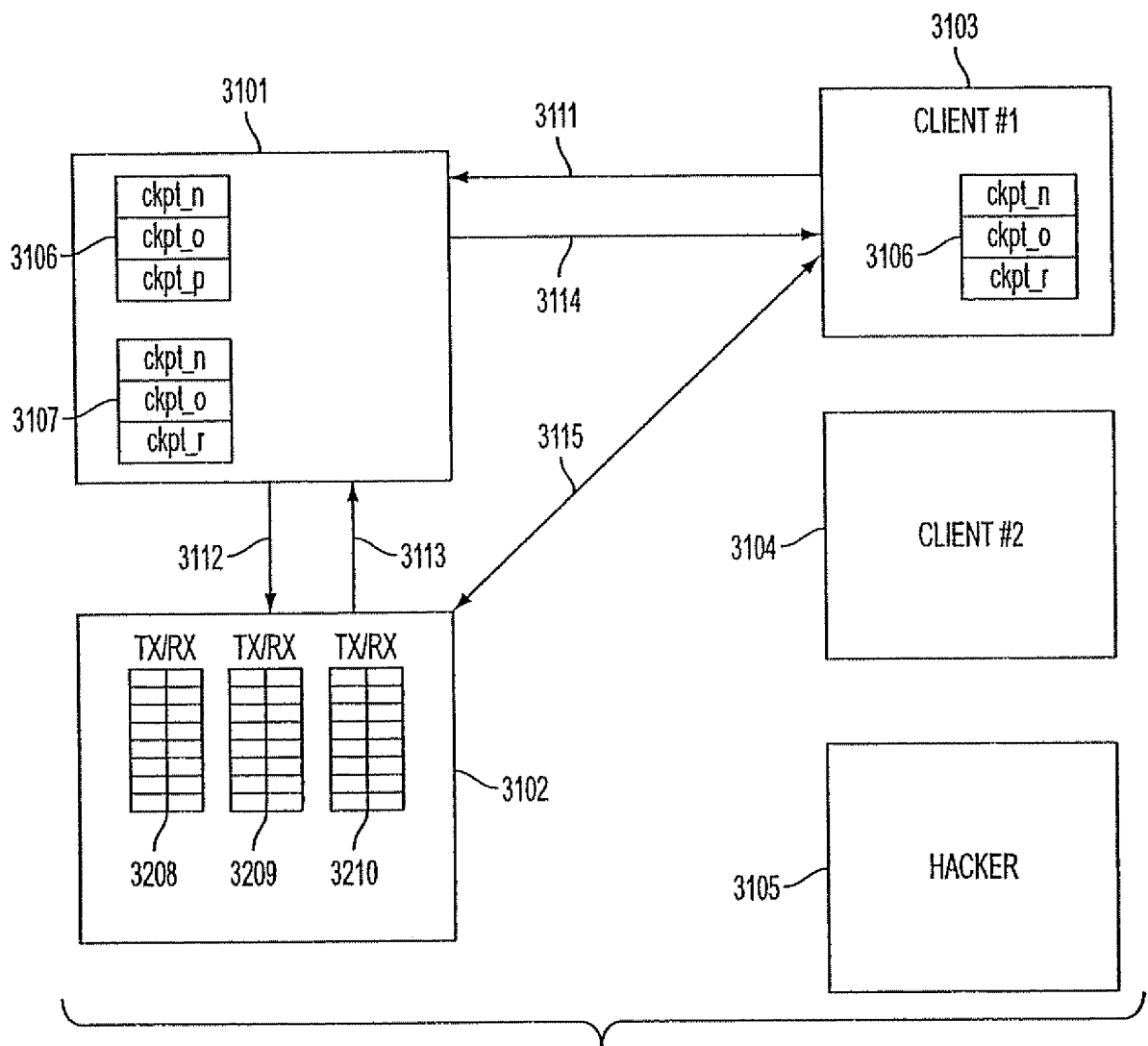


FIG. 31

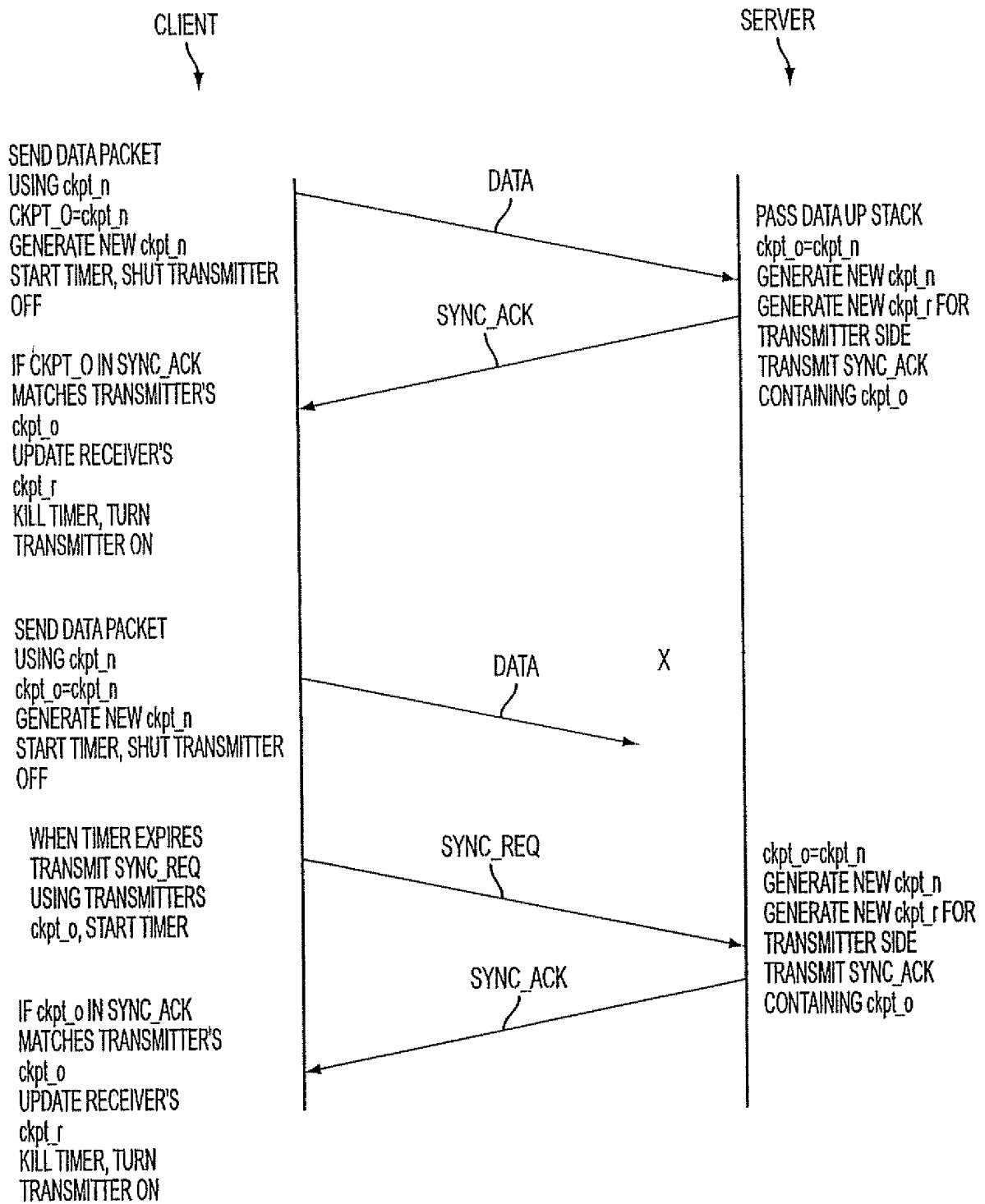


FIG. 32

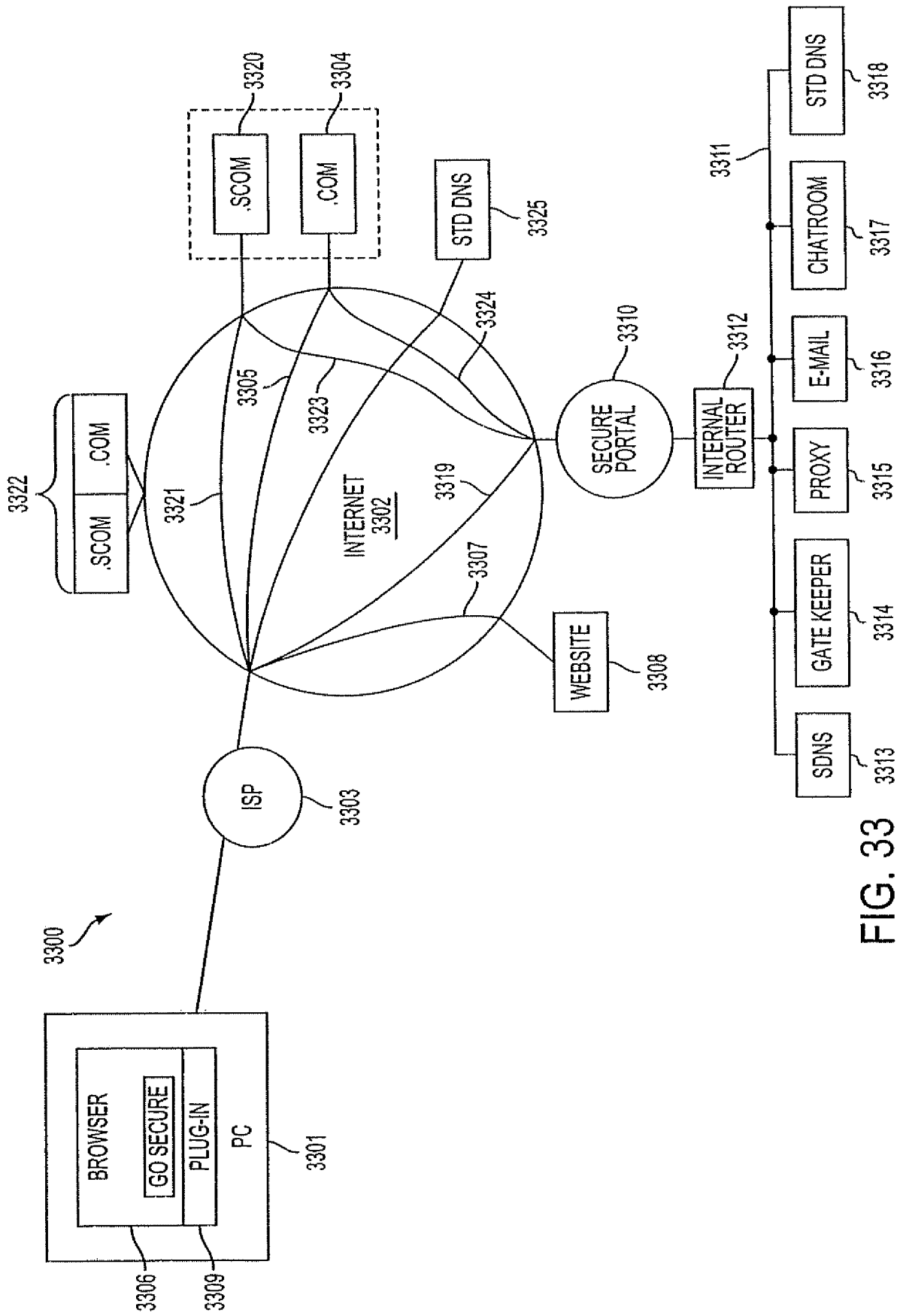


FIG. 33

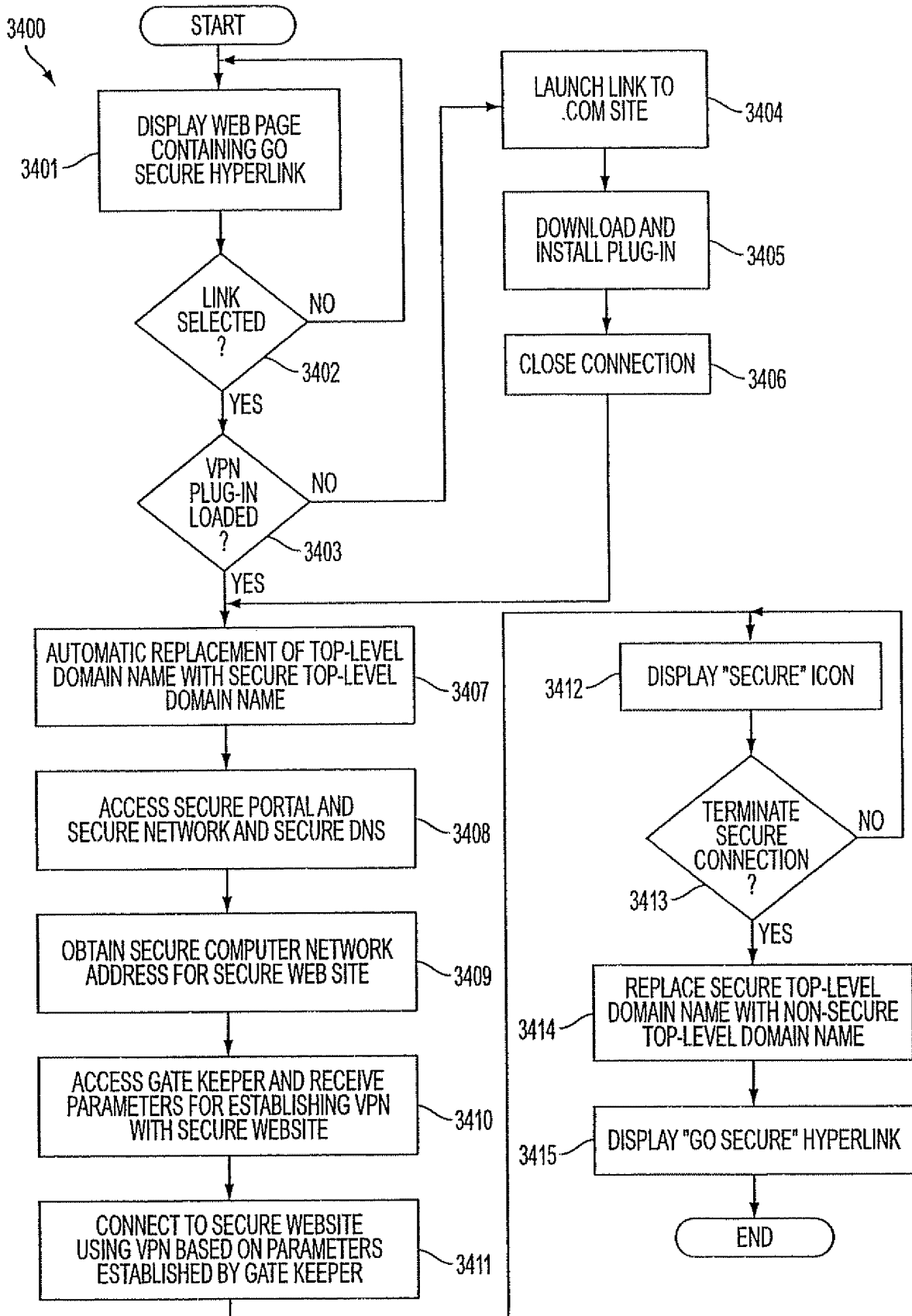


FIG. 34

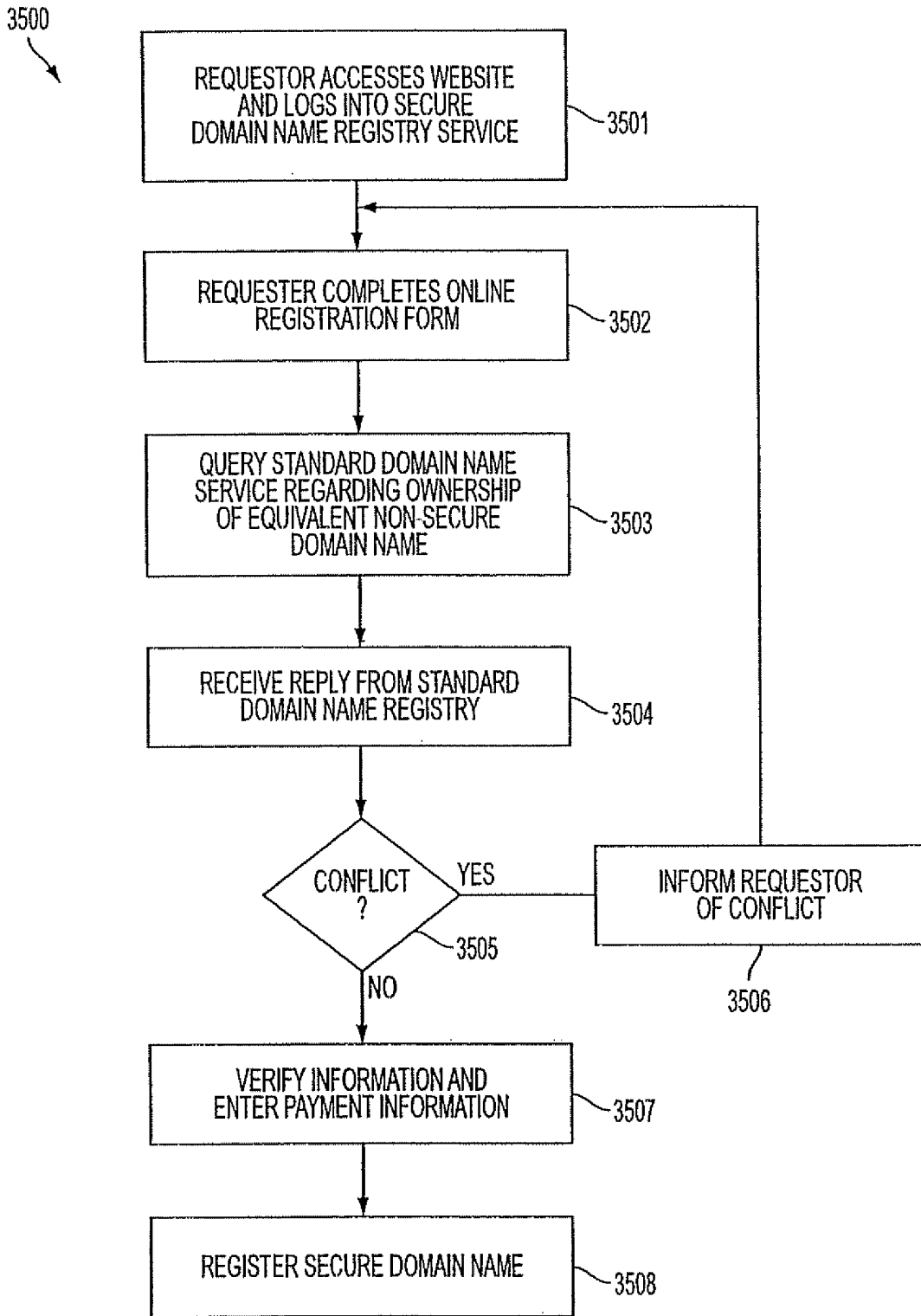


FIG. 35

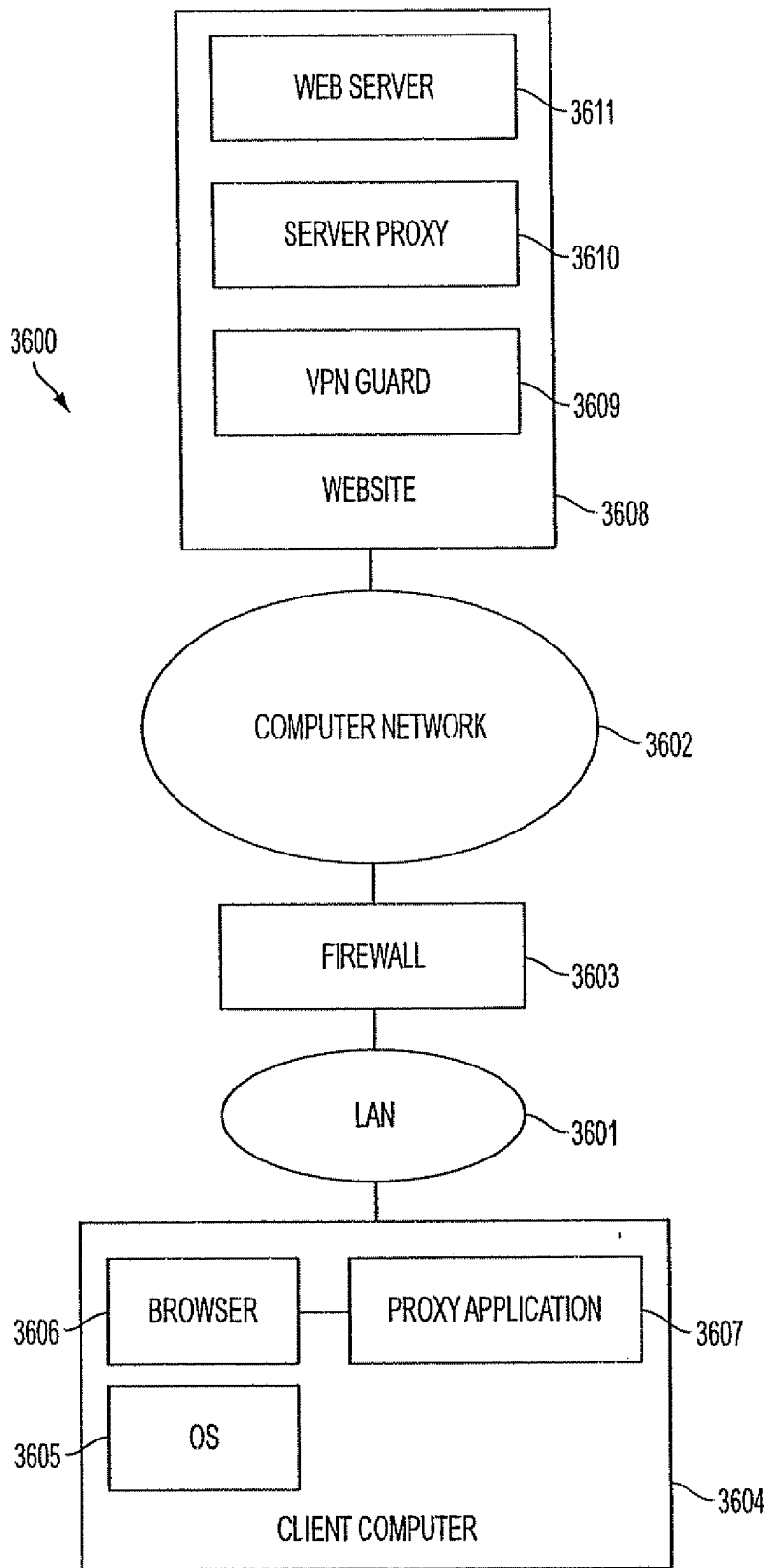


FIG. 36

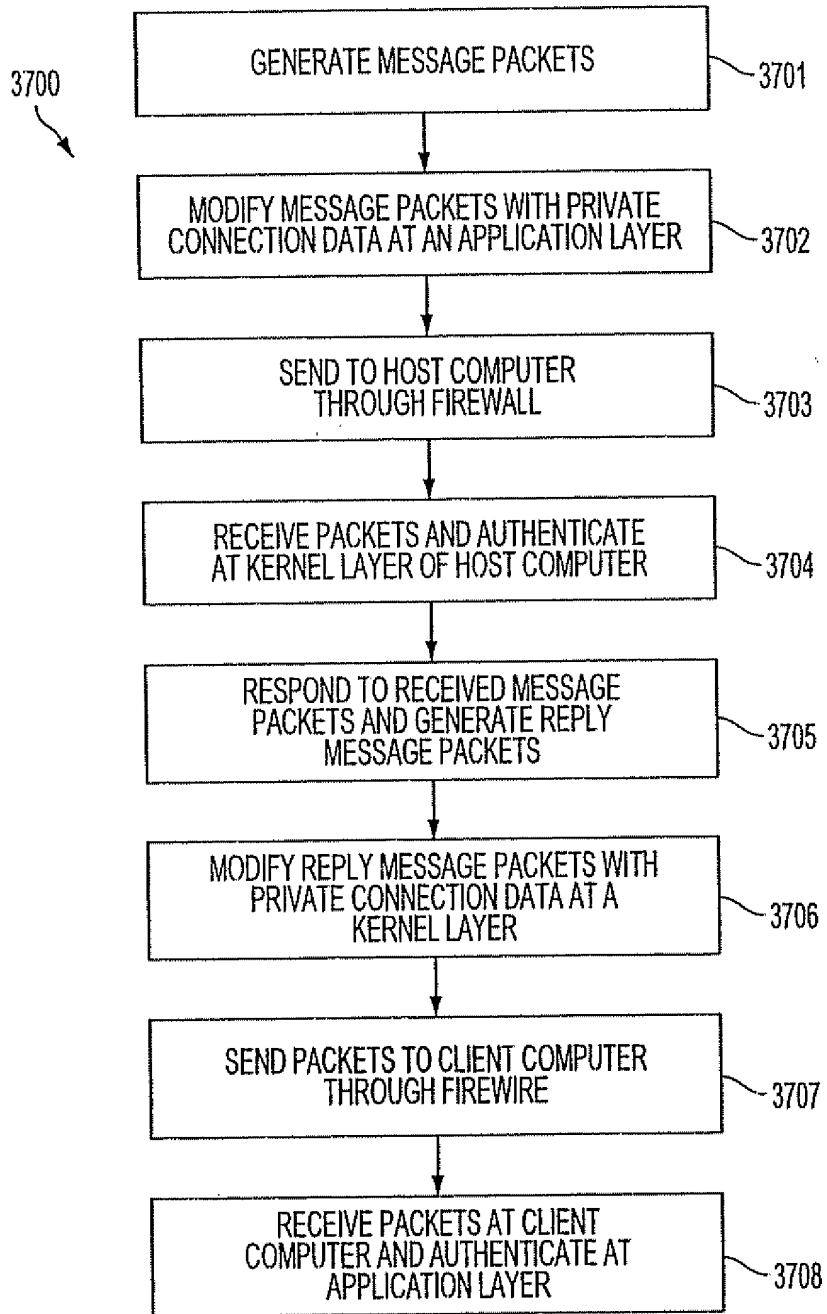


FIG. 37

Electronic Patent Application Fee Transmittal

Application Number:				
Filing Date:				
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK			
First Named Inventor/Applicant Name:	Victor Larson			
Filer:	Atabak R Royae			
Attorney Docket Number:	77580-66 (VRNK-1CP2DVCN2)			
Filed as Large Entity				
Utility Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Utility application filing	1011	1	300	300
Utility Search Fee	1111	1	500	500
Utility Examination Fee	1311	1	200	200
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 (\$)				1000

Electronic Acknowledgement Receipt

EFS ID:	2092436
Application Number:	11839987
International Application Number:	
Confirmation Number:	9470
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Atabak R Royae
Filer Authorized By:	
Attorney Docket Number:	77580-66 (VRNK-1CP2DVCN2)
Receipt Date:	16-AUG-2007
Filing Date:	
Time Stamp:	16:34:50
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	\$ 1000
RAM confirmation Number	9646
Deposit Account	501133

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 and 1.17

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal of New Application	Transmittal.pdf	436820 93b16889cf2595db9724433c535b1142f0e2e664	no	4
Warnings:					
Information:					
2	Application Data Sheet	ADS.pdf	373355 c9b6a98134f87484eaf00582f51647184c1bb6ee	no	4
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
3		Application.pdf	6725611 4cb02e4fb216931ef9e563dodd47d1eaf710c19e	yes	118
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Specification		1	76	
	Claims		77	77	
	Abstract		78	78	
	Drawings		79	118	
Warnings:					
Information:					
4	Fee Worksheet (PTO-06)	fee-info.pdf	8429 da5ba19ab21758f0b1badf8d94b5143fda4bb193	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			7544215		

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.

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 11/839,987					
APPLICATION AS FILED – PART I (Column 1) (Column 2)					SMALL ENTITY		OR		OTHER THAN SMALL ENTITY	
FOR		NUMBER FILED	NUMBER EXTRA		RATE (\$)	FEE (\$)			RATE (\$)	FEE (\$)
BASIC FEE (37 CFR 1.16(a), (b), or (c))										300
SEARCH FEE (37 CFR 1.16(k), (l), or (m))										500
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))										200
TOTAL CLAIMS (37 CFR 1.16(i))		1	minus 20 = *		X\$ 25=				X\$50=	
INDEPENDENT CLAIMS (37 CFR 1.16(h))		1	minus 3 = *		X\$100=				X\$200=	
APPLICATION SIZE FEE (37 CFR 1.16(s))		If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR								
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))						N/A				N/A
					TOTAL				TOTAL	1000
* If the difference in column 1 is less than zero, enter "0" in column 2.										
APPLICATION AS AMENDED – PART II (Column 1) (Column 2) (Column 3)					SMALL ENTITY		OR		OTHER THAN SMALL ENTITY	
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)			RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	*	Minus **	=	X =				X =	
	Independent (37 CFR 1.16(h))	*	Minus ***	=	X =				X =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					N/A				N/A
					TOTAL ADD'T FEE				TOTAL ADD'T FEE	
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)			RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	*	Minus **	=	X =				X =	
	Independent (37 CFR 1.16(h))	*	Minus ***	=	X =				X =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					N/A				N/A
					TOTAL ADD'T FEE				TOTAL ADD'T 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.										

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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



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

Table with 7 columns: APPLICATION NUMBER, FILING or 371(c) DATE, GRP ART UNIT, FIL FEE REC'D, ATTY.DOCKET.NO, TOT CLAIMS, IND CLAIMS. Row 1: 11/839,987, 08/16/2007, 2157, 1000, 077580-0066 (VRNK-1CP2DVC), 1, 1

CONFIRMATION NO. 9470

FILING RECEIPT

23630
MCDERMOTT WILL & EMERY LLP
28 STATE STREET
BOSTON, MA02109-1775

Date Mailed: 09/21/2007

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 write to the Office of Initial Patent Examination's Filing Receipt Corrections. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections

Applicant(s)

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

Assignment For Published Patent Application

VirnetX, Inc., Scotts Valley, CA

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 11/679,416 02/27/2007
which is a CON of 10/702,486 11/07/2003 PAT 7,188,180
which is a DIV of 09/558,209 04/26/2000 ABN
which is a CIP of 09/504,783 02/15/2000 PAT 6,502,135
which is a CIP of 09/429,643 10/29/1999 PAT 7,010,604
which claims benefit of 60/106,261 10/30/1998
and claims benefit of 60/137,704 06/07/1999

Foreign Applications

If Required, Foreign Filing License Granted:

Projected Publication Date: To Be Determined - pending completion of Missing Parts

Non-Publication Request: No

Early Publication Request: No

Title

METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN
COMPUTERS OF VIRTUAL PRIVATE NETWORK

Preliminary Class

709

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

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

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 Assets Control, 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).

McDermott Will & Emery

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

Strategic alliance with MWE China Law Offices (Shanghai)

RECEIVED
CENTRAL FAX CENTER

OCT 04 2007

FACSIMILE

Date: October 4, 2007

Time Sent:

To:	Company:	Facsimile No:	Telephone No:
Commissioner for Patents	U.S. Patent and Trademark Office	1.571.273.8300	
From:	Toby H. Kusmer, P.C.	<i>Direct Phone:</i>	617.535.4065
<i>E-Mail:</i>	tkusmer@mwe.com	<i>Direct Fax:</i>	617.535.3800
<i>Sent By:</i>	Cynthia Joseph	<i>Direct Phone:</i>	617.535.4111
<i>Client/Matter/Tkpr:</i>	77580-066/5496	<i>Original to Follow by Mail:</i>	No
		<i>Number of Pages, Including Cover:</i>	2

Re: In re Application of: Victor Larson, et al.
Serial No.: 11/839,987
Filing Date: August 16, 2007
Title: Method For Establishing Secure Communications Link Between Computers Of Virtual Private Network
Docket No.: 77580-066 (VRNK-1CP2DVCN2)

Message:

Please enter the attached Status Inquiry.

The information contained in this facsimile message is legally privileged and confidential information intended only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, or copy of this facsimile is strictly prohibited. If you have received this facsimile in error, please notify us immediately by telephone and return the original message to us at the below address by mail. Thank you.

IF YOU DO NOT RECEIVE ALL OF THE PAGES, PLEASE CALL AS SOON AS POSSIBLE.

Main Facsimile: 617.535.3800 Facsimile Operator: 617.535.4000

U.S. practice conducted through McDermott Will & Emery LLP.
28 State Street Boston, Massachusetts 02109-1775 Telephone: 617.535.4000

BST99 1553063-1.077580.0066

PAGE 1/2 * RCVD AT 10/4/2007 12:26:57 PM [Eastern Daylight Time] * SVR:USPTO-EFXXRF-5/14 * DNIS:2738300 * CSID:1 617 535 3800 * DURATION (mm-ss):00-44

RECEIVED
CENTRAL FAX CENTER

OCT 04 2007
PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Victor Larson, et al.
Serial No: 11/839,987
Filing Date: August 16, 2007
Title: Method For Establishing Secure Communications Link
Between Computers Of Virtual Private Network

Group Art Unit:
Confirmation No.: 9470
Docket No: 77580-066 (VRNK-1CP2DVCN2)

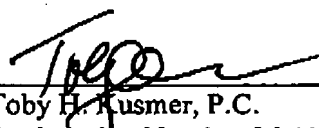
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Sir:

STATUS INQUIRY

Applicants make a request as to the status of the above-identified application and for information as to when they might expect to receive an Office Action.

Respectfully submitted,

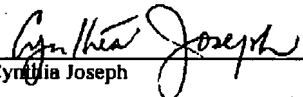


Toby H. Kusmer, P.C.
Registration Number 26,418
McDermott Will & Emery LLP
28 State Street
Boston, Massachusetts 02109-1775
Telephone: (617) 535-4065
Facsimile: (617) 535-3800
e-mail: tkusmer@mwe.com

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence is being facsimile transmitted, via Facsimile No. 571.273.8300, to the U.S. Patent and Trademark Office and is addressed to: Commissioner For Patents, P. O. Box 1450, Alexander, VA 22313-1450 on the date indicated below.

Date: October 4, 2007



Cynthia Joseph

BST99 1553752-1.077580.0066



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

Table with 4 columns: APPLICATION NUMBER, FILING OR 371(C) DATE, FIRST NAMED APPLICANT, ATTY. DOCKET NO./TITLE

11/839,987

08/16/2007

Victor Larson

077580-0066

(VRNK-1CP2DVC

CONFIRMATION NO. 9470

FORMALITIES LETTER

23630
MCDERMOTT WILL & EMERY LLP
28 STATE STREET
BOSTON, MA 02109-1775



Date Mailed: 10/19/2007

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given TWO MONTHS from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment.

- The oath or declaration is missing. A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required. Note: If a petition under 37 CFR 1.47 is being filed, an oath or declaration in compliance with 37 CFR 1.63 signed by all available joint inventors, or if no inventor is available by a party with sufficient proprietary interest, is required.

The applicant needs to satisfy supplemental fees problems indicated below.

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

- To avoid abandonment, a surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of \$130 for a non-small entity, must be submitted with the missing items identified in this notice.

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is \$130 for a non-small entity

- \$130 Surcharge.

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.

/anguyen/

Office of Initial Patent Examination (571) 272-4000 or 1-800-PTO-9199



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

Table with 7 columns: APPLICATION NUMBER, FILING or 371(c) DATE, GRP ART UNIT, FIL FEE REC'D, ATTY DOCKET NO, TOT CLAIMS, IND CLAIMS. Row 1: 11/839,987, 08/16/2007, 2157, 1000, 077580-0066 (VRNK-1CP2DVC), 1, 1

CONFIRMATION NO. 9470

23630
MCDERMOTT WILL & EMERY LLP
28 STATE STREET
BOSTON, MA 02109-1775

FILING RECEIPT



Date Mailed: 10/19/2007

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 write to the Office of Initial Patent Examination's Filing Receipt Corrections. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections

Applicant(s)

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

Assignment For Published Patent Application

VirnetX, Inc., Scotts Valley, CA

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 11/679,416 02/27/2007
which is a CON of 10/702,486 11/07/2003 PAT 7,188,180
which is a DIV of 09/558,209 04/26/2000 ABN
which is a CIP of 09/504,783 02/15/2000 PAT 6,502,135
which is a CIP of 09/429,643 10/29/1999 PAT 7,010,604
which claims benefit of 60/106,261 10/30/1998
and claims benefit of 60/137,704 06/07/1999

Foreign Applications

Projected Publication Date: To Be Determined - pending completion of Missing Parts

Non-Publication Request: No

Early Publication Request: No

Title

METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

Preliminary Class

709

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

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

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 Assets Control, 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).

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 <i>(to be used for all correspondence after initial filing)</i>	Application Number	11/839,987	
	Filing Date	August 16, 2007	
	First Named Inventor	Victor Larson	
	Art Unit	2157	
	Examiner Name	Not Yet Assigned	
Total Number of Pages in This Submission	3	Attorney Docket Number	077580-0066 (VRNK-1CP2DVCN2)

ENCLOSURES (Check all that apply)		
<input type="checkbox"/> Fee Transmittal Form	<input type="checkbox"/> Drawing(s)	<input type="checkbox"/> After Allowance Communication to TC
<input type="checkbox"/> Fee Attached	<input type="checkbox"/> Licensing-related Papers	<input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences
<input type="checkbox"/> Amendment/Reply	<input type="checkbox"/> Petition	<input type="checkbox"/> Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
<input type="checkbox"/> After Final	<input type="checkbox"/> Petition to Convert to a Provisional Application	<input type="checkbox"/> Proprietary Information
<input type="checkbox"/> Affidavits/declaration(s)	<input checked="" type="checkbox"/> Power of Attorney, Revocation Change of Correspondence Address	<input type="checkbox"/> Status Letter
<input type="checkbox"/> Extension of Time Request	<input type="checkbox"/> Terminal Disclaimer	<input type="checkbox"/> Other Enclosure(s) (please Identify below):
<input type="checkbox"/> Express Abandonment Request	<input type="checkbox"/> Request for Refund	
<input type="checkbox"/> Information Disclosure Statement	<input type="checkbox"/> CD, Number of CD(s) _____	
<input type="checkbox"/> Certified Copy of Priority Document(s)	<input type="checkbox"/> Landscape Table on CD	
<input type="checkbox"/> Reply to Missing Parts/ Incomplete Application	<input type="checkbox"/> Remarks	
<input type="checkbox"/> Reply to Missing Parts under 37 CFR 1.52 or 1.53	No fees are believed to be due with the filing of this paper; however, the commissioner is hereby authorized to charge any necessary fees in relation to this filing to Deposit Account No. 50-1133.	

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	McDERMOTT WILL & EMERY LLP		
Signature	/ATABAK R. ROYAE/		
Printed name	ATABAK R. ROYAE		
Date	October 22, 2007	Reg. No.	59,037

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	/ATABAK R. ROYAE/		
Typed or printed name	ATABAK R. ROYAE	Date	October 22, 2007

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

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

I hereby appoint:

Practitioners associated with the Customer

23,630

OR

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

Name	Registration Number		Name	Registration Number

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

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

The address associated with Customer

23,630

OR

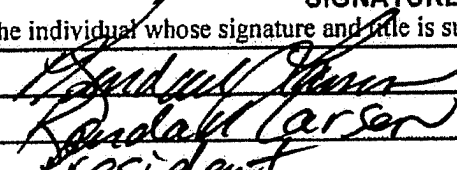
<input checked="" type="checkbox"/> Firm or Individual Name	McDermott Will & Emery LLP		
Address	28 State Street		
City	Boston	State	MA Zip 02109
Country	U.S.A.		
Telephone	(617) 535-4065	Email	tkusmer@mwe.com

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

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

SIGNATURE of Assignee of Record

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

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

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

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: VIRNETX, INC.

Application No./Patent No.: 11/839,987

Filed/Issue Date: AUGUST 16, 2007

Entitled: **METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK**

VIRNETX, INC

, a CORPORATION

(Name of Assignee)

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

states that it is:

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

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

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

OR

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

1. From: Victor Larson, et al. To: Science Applications International Corporation
 The document was recorded in the United States Patent and Trademark Office at
 Reel 019722, Frame 0230, or for which a copy thereof is attached.

2. From: Science Applications International Corporation To: VirnetX, Inc
 The document was recorded in the United States Patent and Trademark Office at
 Reel 019722, Frame 0506, or for which a copy thereof is attached.

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

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

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

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

The undersigned hereby is authorized to act on behalf of the assignee.

[Signature]
Signature

10/19/07
Date

Renda M. Larsen
Printed or Typed Name

831.600.5698
Telephone number

President
Title

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

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

Electronic Acknowledgement Receipt

EFS ID:	2348601
Application Number:	11839987
International Application Number:	
Confirmation Number:	9470
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Atabak R Royae
Filer Authorized By:	
Attorney Docket Number:	077580-0066 (VRNK-1CP2DVC)
Receipt Date:	22-OCT-2007
Filing Date:	16-AUG-2007
Time Stamp:	10:59:46
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	Transmittal_66.pdf	46827 <small>beb0b3290181f710c7c58f519ed835f6c0211cd</small>	no	1

Warnings:

Information:					
2	Power of Attorney	POA_66.pdf	359318	no	2
			6c865b274385004d24baad9ccc9714e8 8ca1d038		

Warnings:

Information:

Total Files Size (in bytes):	406145
-------------------------------------	--------

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

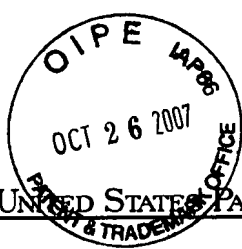
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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.



RECEIVED
OCT 22 2007

10-29-07

F77

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
11/839,987	08/16/2007	Victor Larson	077580-0066 (VRNK-1CP2DVC)

CONFIRMATION NO. 9470

FORMALITIES LETTER

23630
MCDERMOTT WILL & EMERY LLP
28 STATE STREET
BOSTON, MA 02109-1775



0C000000026314599

Date Mailed: 10/19/2007

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. 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 oath or declaration is missing.
A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.
Note: If a petition under 37 CFR 1.47 is being filed, an oath or declaration in compliance with 37 CFR 1.63 signed by all available joint inventors, or if no inventor is available by a party with sufficient proprietary interest, is required.

The applicant needs to satisfy supplemental fees problems indicated below.

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

- To avoid abandonment, a surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of **\$130** for a non-small entity, must be submitted with the missing items identified in this notice.

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is **\$130** for a non-small entity

- **\$130** Surcharge.

10/29/2007 ATRINH 00000057 501133 11839987
01 FC:1051 130.00 DA

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.

/anguyen/

Office of Initial Patent Examination (571) 272-4000 or 1-800-PTO-9199



PATENT
077580-0066 (VRNK-1CP2DVCN2)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

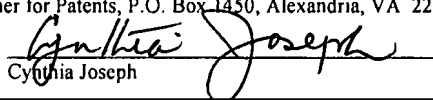
In re Application of: Victor Larson et al.
Serial No: 11/839,987
Filing Date: August 16, 2007
Group Art Unit: 2157
Examiner: To Be Determined
Title: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK
BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
Docket No: 77580-0066 (VRNK-1CP2DVCN2)

CERTIFICATE UNDER 37 CFR § 1.10 OF MAILING BY "EXPRESS MAIL"

EV 942454850 US Date

I hereby certify that this correspondence is being deposited with the United States Postal Services "Express Mail Post Office to Addressee" service under 37 CFR § 1.10 on the date indicated above and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Date: 10-26-07


Cynthia Joseph

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

TRANSMITTAL LETTER

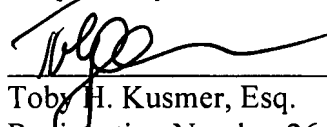
Enclosed herewith for filing in the above-identified patent application please find the following:

1. Response to Notice to File Missing Parts;
2. Statement Under 37 C.F.R. §1.63(d)(1)(iv);
3. Joint Declaration And Power of Attorney for Patent Application;
4. The Change in Power of Attorney and Correspondence Address Under 37 C.F.R. §1.63(d)(4);
5. Copy of Notice to File Missing Parts of Nonprovisional Application; and
6. Return Postcard.

In connection with the foregoing matter, please charge any additional fees which may be due, or credit any overpayment, to Deposit Account Number 50-1133. A duplicate copy of this letter is provided for this purpose.

Date: 10-26-07

Respectfully submitted,



Toby H. Kusmer, Esq.
Registration Number 26,418
McDermott, Will & Emery LLP
28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile: (617) 535-3800
E-mail: tkusmer@mwe.com



PATENT
077580-0066 (VRNK-1CP2DVCN2)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Victor Larson et al.
Serial No: 11/839,987
Filing Date: August 16, 2007
Group Art Unit: 2157
Examiner: To Be Determined
Title: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK
BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
Docket No: 77580-0066 (VRNK-1CP2DVCN2)

CERTIFICATE UNDER 37 CFR § 1.10 OF MAILING BY "EXPRESS MAIL"

EV 942454850 US Date

I hereby certify that this correspondence is being deposited with the United States Postal Services "Express Mail Post Office to Addressee" service under 37 CFR § 1.10 on the date indicated above and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Date: 10-26-07

Cynthia Joseph

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

RESPONSE TO NOTICE TO FILE MISSING PARTS

Sir:

In response to the Notice to File Missing Parts of Non-Provisional Application, dated October 19, 2007, Applicant submits the required executed Declaration under 37 C.F.R. § 1.63(d)(1)(iv).

The Commissioner is also authorized to charge the surcharge fee of \$130.00 and/or any further fees which may be due, and/or credit any overpayment to Deposit Account Number 50-1133.

Respectfully submitted,
McDERMOTT WILL & EMERY LLP

Date: 10-26-07

Toby H. Kusmer, P.C.
Reg. No. 26,418
28 State Street
Boston, MA 02109-1775
DD Telephone: (617) 535-4065
Facsimile: (617) 535-3800
e-mail: tkusmer@mwe.com



PATENT
077580-0066 (VRNK-1CP2DVCN2)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

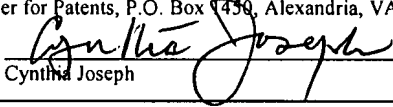
In re Application of: Victor Larson et al.
Serial No: 11/839,987
Filing Date: August 16, 2007
Group Art Unit: 2157
Examiner: To Be Determined
Title: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK
BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
Docket No: 77580-0066 (VRNK-1CP2DVCN2)

CERTIFICATE UNDER 37 CFR § 1.10 OF MAILING BY "EXPRESS MAIL"

EV 942454850 US Date

I hereby certify that this correspondence is being deposited with the United States Postal Services "Express Mail Post Office to Addressee" service under 37 CFR § 1.10 on the date indicated above and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Date: 10.26.07


Cynthia Joseph

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

THE CHANGE IN POWER OF ATTORNEY
AND CORRESPONDENCE ADDRESS UNDER 37 C.F.R. § 1.63 (d)(4)

Dear Sir:

In accordance with 37 C.F.R. § 1.63 (d)(4) and pursuant to the Power of Attorney and Change of Correspondence Address filed on October 22, 2007, Applicants in the above-identified patent application have revoked all powers of attorney previously given in connection with the prior application and have appointed the following attorneys, with full power of substitution, to transact all business in the Patent and Trademark Office connected therewith:

All attorneys associated with CUSTOMER NUMBER 23630

BST99 1555850-1.077580.0066


It is requested that all correspondence regarding this patent application be directed to:

Toby H. Kusmer, P.C.
McDermott Will & Emery LLP
28 State Street
Boston, Massachusetts 02109-1775
Telephone: (617) 535-4065
Facsimile: (617) 535-3800
E-mail: tkusmer@mwe.com

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Date: 10.26.07



Toby H. Kusmer, P.C.
Reg. No. 26,418
28 State Street
Boston, MA 02109-1775
DD Telephone: (617) 535-4065
Facsimile: (617) 535-3800
e-mail: tkusmer@mwe.com



PATENT
077580-0066 (VRNK-1CP2DVCN2)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of: Victor Larson et al.
Serial No: 11/839,987
Filing Date: August 16, 2007
Group Art Unit: 2157
Examiner: To Be Determined
Title: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK
BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
Docket No: 77580-0066 (VRNK-1CP2DVCN2)

CERTIFICATE UNDER 37 CFR § 1.10 OF MAILING BY "EXPRESS MAIL"
EV 942454850 US Date

I hereby certify that this correspondence is being deposited with the United States Postal Services "Express Mail Post Office to Addressee" service under 37 CFR § 1.10 on the date indicated above and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Date: 10.26.07

Cynthia Joseph
Cynthia Joseph

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

STATEMENT UNDER 37 C.F.R. § 1.63(d)(1)(iv)

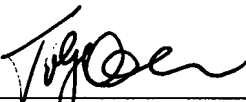
Sir:

In accordance with 37 C.F.R. § 1.63(d)(1)(iv), for the above-identified continuation application, Applicants hereby submit a copy of the original Declaration filed in the prior application. The above-identified application is a continuation of U.S. Application Serial No. 11/679,416, filed February 27, 2007, which is a continuation of U.S. Application Serial No. 10/702,486, filed November 7, 2003, which is divisional of U.S. Application Serial No. 09/558,209, filed April 26, 2000, which is a continuation-in-part of U.S. Application No. 09/504,783, filed February 15, 2000, which is a continuation-in-part of U.S. Application No. 09/429,643, filed October 29, 1999, which claims the benefit under 35 U.S.C. 119(e) to U.S. Provisional Application Nos. 60/106,261, filed October 30, 1998, and 60/137,704, filed June 7, 1999.

The Commissioner is hereby authorized to charge any fees due with the filing of this paper to Deposit Account No. 50-1133.

Respectfully submitted,
McDERMOTT WILL & EMERY LLP

Date: 10-26-07



Toby H. Kusmer, P.C.
Reg. No. 26,418
28 State Street
Boston, MA 02109-1775
DD Telephone: (617) 535-4065
Facsimile: (617)535-3800
e-mail: tkusmer@mwe.com

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 METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK, 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:

Banner & Witcoff Ref. No. 000479.00112
 Client Ref. No. 10006-Div. (1)

Application Serial No.	Date of Filing (Day, Month, Year)	Status — Patented, Pending, Abandoned
09/558,209	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 11/6/03
 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 A. Short III* Date 10/27/03
 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 *Edmund Colby Menger* Date 11/5/03
 Full Name of Third Inventor Menger 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 *Michael Williamson* Date 11/9/03
 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



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

Table with 7 columns: APPLICATION NUMBER, FILING or 371(c) DATE, GRP ART UNIT, FIL FEE REC'D, ATTY DOCKET NO, TOT CLAIMS, IND CLAIMS. Row 1: 11/839,987, 08/16/2007, 2157, 1130, 77580-0066 (VRNK-ICP2DVCN), 1, 1

CONFIRMATION NO. 9470

UPDATED FILING RECEIPT

23630
MCDERMOTT WILL & EMERY LLP
28 STATE STREET
BOSTON, MA 02109-1775



Date Mailed: 11/08/2007

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 write to the Office of Initial Patent Examination's Filing Receipt Corrections. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections

Applicant(s)

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

Assignment For Published Patent Application

VirnetX, Inc., Scotts Valley, CA

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

Domestic Priority data as claimed by applicant

This application is a CON of 11/679,416 02/27/2007
which is a CON of 10/702,486 11/07/2003 PAT 7,188,180
which is a DIV of 09/558,209 04/26/2000 ABN
which is a CIP of 09/504,783 02/15/2000 PAT 6,502,135
which is a CIP of 09/429,643 10/29/1999 PAT 7,010,604
which claims benefit of 60/106,261 10/30/1998
and claims benefit of 60/137,704 06/07/1999

Foreign Applications

Projected Publication Date: To Be Determined - pending completion of Security Review

Non-Publication Request: No

Early Publication Request: No

Title

METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

Preliminary Class

709

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

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

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 Assets Control, 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).

DEPARTMENT OF DEFENSE
ACCESS ACKNOWLEDGEMENT / SECRECY ORDER RECOMMENDATION
FOR PATENT APPLICATION

Application Serial No: DP11839987 Filing Date: Date Referred: 09/12/2007

I hereby acknowledge that the Department of Defense reviewers has inspected this application in administration of 35 USC 181 on behalf of the Agencies/Commands specified below. DoD reviewers will not divulge any information from this application for any purpose other than administration of 35 USC 181.

Defense Agency	Recommendation	Reviewer Name	Date Reviewed
Army	Secrecy Not Recommended	Herbert Rose	02/19/2008
NSA	Secrecy Not Recommended	Eric Froehlich	10/09/2007

<i>Type of Recommendations:</i> <i>SNR: Secrecy Not Recommended</i> <i>SR: Secrecy Recommended</i> <i>NC: No Comment</i>
--

Instructions to Reviewers:

1. All DoD personnel reviewing this application will be listed on this form regardless of whether they are making a secrecy order recommendation.
2. This form will be forwarded to USPTO once all assigned DoD entities have provided their secrecy order recommendation.

Time for Completion of Review:

Pursuant to 35 USC 184, the subject matter of this applicaiton may be filed in a foreign country for the purposed of filing a patent application without a license anytime after the expriation of six (6) months from filing date unless the application becomes the subject of a secrecy order.

<i>The USPTO publishes patent application at 18 months from the earliest claimed filing date. The USPTO will delay the publication of a patent application made available to a defense agency under 35 USC 181 until no earlier than 6 months from the filing date or 90 days from the date of referral to that agency. This application will be cleared for publication 6 months from the filing date or 90 days from the above Date Referred, whichever is later, unless a response is provided to the USPTO regarding the necessary recommendations as to the imposition of a secrecy order.</i>

DoD Completion of Review: Final Forwarded to USPTO: 02/19/2008 By: Oksana Nesterczuk
--



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
11/839,987	08/16/2007	Victor Larson	77580-0066 (VRNK-1CP2DVCN)

CONFIRMATION NO. 9470

23630
MCDERMOTT WILL & EMERY LLP
28 STATE STREET
BOSTON, MA02109-1775

Date Mailed. 05/29/2008

NOTICE OF NEW OR REVISED PROJECTED PUBLICATION DATE

The above-identified application has a new or revised projected publication date. The current projected publication date for this application is 09/04/2008. If this is a new projected publication date (there was no previous projected publication date), the application has been cleared by Licensing & Review or a secrecy order has been rescinded and the application is now in the publication queue.

If this is a revised projected publication date (one that is different from a previously communicated projected publication date), the publication date has been revised due to processing delays in the USPTO or the abandonment and subsequent revival of an application. The application is anticipated to be published on a date that is more than six weeks different from the originally-projected publication date.

More detailed publication information is available through the private side of Patent Application Information Retrieval (PAIR) System. The direct link to access PAIR is currently <http://pair.uspto.gov>. Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Questions relating to this Notice should be directed to the Office of Patent Publication at 1-888-786-0101.

PART 1 - ATTORNEY/APPLICANT COPY



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

Table with 4 columns: APPLICATION NUMBER, FILING OR 371(C) DATE, FIRST NAMED APPLICANT, ATTY. DOCKET NO./TITLE. Row 1: 11/839,987, 08/16/2007, Victor Larson, 77580-0066 (VRNK-1CP2DVCN)

23630
MCDERMOTT WILL & EMERY LLP
28 STATE STREET
BOSTON, MA 02109-1775

CONFIRMATION NO. 9470
PUBLICATION NOTICE



Title:METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

Publication No.US-2008-0216168-A1
Publication Date:09/04/2008

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		11839987	
	Filing Date		2007-08-16	
	First Named Inventor	Larson, et al.		
	Art Unit			
	Examiner Name			
	Attorney Docket Number		77580-66(VR NK-1CP2DVCN2)	

U.S.PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1	5384848		1995-01-00	Kikuchi		
	2	6223287		2001-04-00	Douglas, et al.		

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS							Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1						

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² j	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							<input type="checkbox"/>

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS								Remove
---------------------------------	--	--	--	--	--	--	--	--------

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		11839987	
	Filing Date		2007-08-16	
	First Named Inventor	Larson, et al.		
	Art Unit			
	Examiner Name			
	Attorney Docket Number		77580-66(VRNK-1CP2DVCN2)	

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		<input type="checkbox"/>

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	11839987		
Filing Date	2007-08-16		
First Named Inventor	Larson, et al.		
Art Unit			
Examiner Name			
Attorney Docket Number	77580-66(VR NK-1CP2DVCN2)		

CERTIFICATION STATEMENT

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

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

None

SIGNATURE

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

Signature	/THK/	Date (YYYY-MM-DD)	2008-12-16
Name/Print	Toby H. Kusmer	Registration Number	26,418

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

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

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

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

Electronic Acknowledgement Receipt

EFS ID:	4461586
Application Number:	11839987
International Application Number:	
Confirmation Number:	9470
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Erin Shea
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-0066 (VRNK-1CP2DVCN)
Receipt Date:	16-DEC-2008
Filing Date:	16-AUG-2007
Time Stamp:	10:57:34
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) Filed (SB/08)	77580_066_US_IDS_Form__SB _08a.pdf	608040 <small>6e4c21c8807e8a4f9dae375c6ef26e6e1bd78efd</small>	no	4

Warnings:

Information:

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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		11839987	
	Filing Date		2007-08-16	
	First Named Inventor	Larson, et al.		
	Art Unit			
	Examiner Name			
	Attorney Docket Number		77580-66(VR NK-1CP2DVCN2)	

U.S.PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1	5303302		1994-04-12	Burrows		
	2	5629984		1997-05-13	McManis		

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS							Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1						

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² j	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							<input type="checkbox"/>

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS								Remove
---------------------------------	--	--	--	--	--	--	--	--------

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		11839987	
	Filing Date		2007-08-16	
	First Named Inventor	Larson, et al.		
	Art Unit			
	Examiner Name			
	Attorney Docket Number		77580-66(VRNK-1CP2DVCN2)	

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		<input type="checkbox"/>

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11839987
	Filing Date	2007-08-16
	First Named Inventor	Larson, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	77580-66(VRNK-1CP2DVCN2)

CERTIFICATION STATEMENT

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

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

- See attached certification statement.
- Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.
- None

SIGNATURE

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

Signature	/ARR/	Date (YYYY-MM-DD)	2009-01-22
Name/Print	Atabak R. Royae	Registration Number	59,037

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

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

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

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

Electronic Acknowledgement Receipt

EFS ID:	4657156
Application Number:	11839987
International Application Number:	
Confirmation Number:	9470
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Atabak R Royaee/Erin Shea
Filer Authorized By:	Atabak R Royaee
Attorney Docket Number:	77580-0066 (VRNK-1CP2DVCN)
Receipt Date:	22-JAN-2009
Filing Date:	16-AUG-2007
Time Stamp:	14:36:46
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) Filed (SB/08)	77580_066_US_IDS_Form__SB _08a.pdf	607962 <small>819d0f653c9c395ebd287d3da1bc5f98156 d07e4</small>	no	4

Warnings:

Information:

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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		11839987	
	Filing Date		2007-08-16	
	First Named Inventor	Larson, et al.		
	Art Unit			
	Examiner Name			
	Attorney Docket Number		77580-66(VRNK-1CP2DVCN2)	

U.S.PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1	5771239		1998-06-23	Moroney, et al.		

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS							Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1						

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² j	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							<input type="checkbox"/>

If you wish to add additional Foreign Patent Document citation information please click the Add button. Add

NON-PATENT LITERATURE DOCUMENTS				Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.		T ⁵

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		11839987	
	Filing Date		2007-08-16	
	First Named Inventor	Larson, et al.		
	Art Unit			
	Examiner Name			
	Attorney Docket Number		77580-66(VRNK-1CP2DVCN2)	

	1	FASBENDER, A., et al., Variable and Scalable Security: Protection of Location Information in Mobile IP, IEEE VTS, 46th, 1996, 5 pp.	<input type="checkbox"/>
--	---	---	--------------------------

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	Date Considered
--------------------	-----------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11839987
	Filing Date	2007-08-16
	First Named Inventor	Larson, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	77580-66(VRNK-1CP2DVCN2)

CERTIFICATION STATEMENT

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

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

- See attached certification statement.
- Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.
- None

SIGNATURE

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

Signature	/ARR/	Date (YYYY-MM-DD)	2009-02-24
Name/Print	Atabak R. Royae	Registration Number	59,037

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

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

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

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

Electronic Acknowledgement Receipt

EFS ID:	4848166
Application Number:	11839987
International Application Number:	
Confirmation Number:	9470
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Atabak R Royae/Erin shea
Filer Authorized By:	Atabak R Royae
Attorney Docket Number:	77580-0066 (VRNK-1CP2DVCN)
Receipt Date:	24-FEB-2009
Filing Date:	16-AUG-2007
Time Stamp:	15:32:23
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) Filed (SB/08)	77580_066_US_IDS_Form__SB _08a.pdf	608139 <small>7b7cb0a4e9e20cecbcb13d4837134e94d080b4b</small>	no	4

Warnings:

Information:

2	NPL Documents	VRNK_NPLREFERENCE.PDF	731920 <small>7e1f64823a0ad0d6d42fb2b62ae80e8c05c3f713</small>	no	5
---	---------------	-----------------------	---	----	---

Warnings:

Information:

Total Files Size (in bytes):	1340059
-------------------------------------	---------

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

Table with columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO., EXAMINER, ART UNIT, PAPER NUMBER, MAIL DATE, DELIVERY MODE. Includes application details for Victor Larson and examiner LIM, KRISNA.

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.

Art Unit: 2453

1. Claim 1 is presented for examination.

2. The disclosure is objected to because of the following informalities:
 - (a) On page 1, the text of the first paragraph should be updated with the current status of the cited applications such as U.S. Patent Application Serial No., a filing date, U.S. Patent No., and the issued date. Appropriate correction is required.

3. Claim 1 is rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

At line 3, it is unclear from where a query message is sent. At line 4, it is unclear from where the query message is requesting a secure computer network address. At line 5, it is unclear where the response message is received and from where the response message is received. At line 7, it is unclear from where an access request is sent.

4. .A rejection based on double patenting of the "same invention" type finds its support in the language of 35 U.S.C. 101 which states that "whoever invents or discovers any new and useful process ... may obtain a patent therefor ..." (Emphasis added). Thus, the term "same invention," in this context, means an invention drawn to identical subject matter. See *Miller v. Eagle Mfg. Co.*, 151 U.S. 186 (1894); *In re Ockert*, 245 F.2d 467, 114 USPQ 330 (CCPA 1957); and *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970).

A statutory type (35 U.S.C. 101) double patenting rejection can be overcome by canceling or amending the conflicting claims so they are no longer coextensive in scope. The filing of a terminal disclaimer cannot overcome a double patenting rejection based upon 35 U.S.C. 101.

Art Unit: 2453

5. Claim 1 provisionally rejected under 35 U.S.C. 101 as claiming the same invention as that of claim 1 of copending Application No. 11/679,416. This is a provisional double patenting rejection since the conflicting claims have not in fact been patented.

6. 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).

7. Claim 1 is rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1 of U.S. Patent No. 7,188,180. Although the conflicting claims are not identical, they are not patentably distinct from each other because they are directed to a method of accessing a secure computer network address, comprising steps of: a) receiving a secure domain ...; b) sending a query message to a secure domain ...; c) receiving from the secure domain name center ...;

Art Unit: 2453

and d) sending an access request message to the secure computer network address using a virtual private network communication link. The different is the clarity language of the claim of the parent while the language of the claim of the present application does not.

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

The references are cited in the Form PTO-892 for the applicant's review.

A shortened statutory period for response to this action is set to expire 3 (three) months and 0 (zero) days from the mail date of this letter. Failure to respond within the period for response will result in **ABANDONMENT** of the application (see 35 U.S.C 133, M.P.E.P 710.02, 710.02(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 Monday to Friday from 9:30 AM to 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne, can be reached on 571-272-4001. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KI

June 05, 2009

/Krisna Lim/

Primary Examiner, Art Unit 2453

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	49	((VICTOR) near2 (LARSON)). INV.	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/05 11:06
L2	164	((ROBERT) near2 (SHORT)). INV.	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/05 11:06
L3	27	((EDMUND) near2 (MUNGER)). INV.	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/05 11:06
L4	72	((MICHAEL) near2 (WILLIAMSON)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/05 11:06
L5	242	l1 or l2 or l3 or l4	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:07
L6	242	l5 and ad@ad<"02152000"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:07
L7	43745710	l5 adn ad@ad<="19981030"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:07
L8	242	l5 and ad@<="19981030"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:08
L9	242	l5 and ad@<="02152000"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:09
L10	49	l8 and (secure network address). ti,ab,clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:09
L11	24	l8 and domain.ti,ab,clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:09
L12	15	l11 and (secure adj5 domain).ti, ab,clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:10

L13	3938	(secure same computer same network).ti,ab,clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:11
L14	0	l13 and (secure same domain same name)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:11
L15	110	l13 and (secure same domain same name)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:12
L16	70	l15 and (secure same domain same service)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:14
L17	70	l16 and ad@<="19981030"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:14
L18	70	l17 and (query message secure domain name)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:16

6/ 5/ 09 11:17:42 AM

C:\ Program Files\ USPTO\ EAST\ Bin\ default.wsp

EAST Search History


Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	3938	(secure same computer same network).ti,ab,clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 13:30
L2	110	L1 and (secure same domain same name)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 13:30
L3	70	L2 and (secure same domain same service)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 13:30
L4	70	L3 and ad@<="19981030"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 13:30
L5	70	L4 and (query message secure domain name)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 13:30
L6	27	(secure adj4 computer adj5 network adj5 address)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 13:39
L7	131	(secure adj4 domain adj5 name)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 13:40
L8	131	l7 and ad@<="19981030"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 13:40
L9	4	l7 and @ad<="19981030"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 13:41
L10	16	(secure adj5 computer adj5 network adj5 address).ti,ab,clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 14:08

L11	670	(secure adj6 communication adj6 link).ti,ab,clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 14:27
L12	11	11 and (secure adj6 domain).ti,ab,clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 14:30
S1	49	((VICTOR) near2 (LARSON)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/05 11:06
S2	164	((ROBERT) near2 (SHORT)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/05 11:06
S3	27	((EDMUND) near2 (MUNGER)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/05 11:06
S4	72	((MICHAEL) near2 (WILLIAMSON)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/05 11:06
S5	242	S1 or S2 or S3 or S4	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:07
S6	242	S5 and ad@ad<"02152000"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:07
S7	43745710	S5 adn ad@ad<="19981030"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:07
S8	242	S5 and ad@<="19981030"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:08
S9	242	S5 and ad@<="02152000"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:09
S10	49	S8 and (secure network address).ti,ab,clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:09
S11	24	S8 and domain.ti,ab,clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:09

S12	15	S11 and (secure adj5 domain).ti,ab,clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:10
S13	3938	(secure same computer same network).ti,ab,clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:11
S14	0	S13 and (secure same domain same name)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:11
S15	110	S13 and (secure same domain same name)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:12
S16	70	S15 and (secure same domain same service)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:14
S17	70	S16 and ad@<="19981030"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:14
S18	70	S17 and (query message secure domain name)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:16

6/ 5/ 09 2:37:32 PM

C:\ Documents and Settings\ klim\ My Documents\ EAST\ Workspaces\ 11679416.wsp

Index of Claims 	Application/Control No. 11839987	Applicant(s)/Patent Under Reexamination LARSON ET AL.
	Examiner Krisna Lim	Art Unit 2453

✓	Rejected
=	Allowed


-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

Claims renumbered in the same order as presented by applicant
 CPA
 T.D.
 R.1.47

CLAIM		DATE							
Final	Original	06/05/2009							
	1	✓							

Search Notes 	Application/Control No. 11839987	Applicant(s)/Patent Under Reexamination LARSON ET AL.
	Examiner Krisna Lim	Art Unit 2453

SEARCHED			
Class	Subclass	Date	Examiner
709	225-229, 245	6/5/09	kl

SEARCH NOTES		
Search Notes	Date	Examiner
EAST, Inventors	6/5/09	kl

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

--	--

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		11839987	
	Filing Date		2007-08-16	
	First Named Inventor	Larson, et al.		
	Art Unit			
	Examiner Name			
	Attorney Docket Number		77580-66(VRNK-1CP2DVCN2)	

U.S.PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1	5384848		1995-01-00	Kikuchi		
	2	6223287		2001-04-00	Douglas, et al.		

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS							Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1						

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² j	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							<input type="checkbox"/>

If you wish to add additional Foreign Patent Document citation information please click the Add button. Add

NON-PATENT LITERATURE DOCUMENTS								Remove
---------------------------------	--	--	--	--	--	--	--	--------

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11839987	11839987 - GAU: 2453
	Filing Date	2007-08-16	
	First Named Inventor	Larson, et al.	
	Art Unit		
	Examiner Name		
	Attorney Docket Number	77580-66(VRNK-1CP2DVCN2)	

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		<input type="checkbox"/>

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Krisna Lim/	Date Considered	06/05/2009
--------------------	--------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		11839987	
	Filing Date		2007-08-16	
	First Named Inventor	Larson, et al.		
	Art Unit			
	Examiner Name			
	Attorney Docket Number		77580-66(VRNK-1CP2DVCN2)	

U.S.PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1	5303302		1994-04-12	Burrows		
	2	5629984		1997-05-13	McManis		

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS							Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1						

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² j	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							<input type="checkbox"/>

If you wish to add additional Foreign Patent Document citation information please click the Add button. Add

NON-PATENT LITERATURE DOCUMENTS								Remove
---------------------------------	--	--	--	--	--	--	--	--------

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11839987	11839987 - GAU: 2453
	Filing Date	2007-08-16	
	First Named Inventor	Larson, et al.	
	Art Unit		
	Examiner Name		
	Attorney Docket Number	77580-66(VRNK-1CP2DVCN2)	

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		<input type="checkbox"/>

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Krisna Lim/	Date Considered	06/05/2009
--------------------	--------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		11839987	
	Filing Date		2007-08-16	
	First Named Inventor	Larson, et al.		
	Art Unit			
	Examiner Name			
	Attorney Docket Number		77580-66(VRNK-1CP2DVCN2)	

U.S.PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1	5771239		1998-06-23	Moroney, et al.		

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

U.S.PATENT APPLICATION PUBLICATIONS							Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1						

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							<input type="checkbox"/>

If you wish to add additional Foreign Patent Document citation information please click the Add button

Add

NON-PATENT LITERATURE DOCUMENTS				Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.		T ⁵

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		11839987	11839987 - GAU: 2453	
	Filing Date		2007-08-16		
	First Named Inventor	Larson, et al.			
	Art Unit				
	Examiner Name				
	Attorney Docket Number		77580-66(VR NK-1CP2DVCN2)		

1	FASBENDER, A., et al., Variable and Scalable Security: Protection of Location Information in Mobile IP, IEEE VTS, 46th, 1996, 5 pp.	<input type="checkbox"/>
---	---	--------------------------

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Krisna Lim/	Date Considered	06/05/2009
--------------------	--------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

Subst. for form 1449/PTO SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	11/839,987
				Filing Date	August 16, 2007
				First Named Inventor	Edmund Colby Munger
				Art Unit	2453
				Examiner Name	Lim, Krisna
Sheet	1	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO	Document Number Number-Kind Code ² (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1000	5,311,593	05/10/1994	Carmi	
	A1001	5,511,122	04/23/1996	Atkinson	
	A1003	5,805,803	09/08/1998	Birrell et al.	
	A1004	5,822,434	10/13/1998	Caronni et al.	
	A1005	5,898,830	04/27/1999	Wesinger, Jr. et al.	
	A1006	60/134,547	05/17/1999	Victor Sheymov	
	A1007	60/151,563	08/31/1999	Bryan Whittles	
	A1008	5,950,195	09/07/1999	Stockwell et al.	
	A1009	6,119,171	09/12/2000	Alkhatib	
	A1010	6,937,597	08/30/2005	Rosenberg et al.	
	A1011	7,072,964	07/04/2006	Whittle et al.	
	A1012	09/399,753	09/22/1998	Graig Miller et al.	
	A1013	6,079,020	06/20/2000	Liu	
	A1014	6,173,399	01/09/2001	Gilbrech	
	A1015	6,226,748	05/01/2001	Bots et al.	
	A1016	6,226,751	05/01/2001	Arrow et al.	
	A1017	6,701,437	03/02/2004	Hoke et al.	
	A1018	6,055,574	04/25/2000	Smorodinsky et al.	
	A1019	6,246,670	06/12/2001	Karlsson, et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO	Foreign Patent Document Country Codes - Number + Kind Codes (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No
	B1000	WO 001/17775	03-30-2000	Science Applications International Corporation		Yes	No
	B1001	WO 00/70458	11-23-2000	Comsec Corporation			
	B1002	WO 01/016766	03-08-2001	Science Applications International Corporation			

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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known		
				Application Number	11/839,987	
				Filing Date	August 16, 2007	
				First Named Inventor	Edmund Colby Munger	
				Art Unit	2453	
				Examiner Name	Lim, Krisna	
Sheet	2	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)	
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				
	C998	Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009, VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation,				
	C999	Appendix A of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.				
	C1000	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.				
	C1001	1. P. Mockapetris, "DNS Encoding of Network Names and Other Types," Network Working Group, RFC 1101 (April 1989) (RFC1101, DNS SRV)				
	C1002	DNS-related correspondence dated September 7, 1993 to September 20, 1993. (Pre KX, KX Records) [Due to difficulty locating this reference, a copy has not been provided]				
	C1003	R Atkinson, "An Internetwork Authentication Architecture," Naval Research Laboratory, Center for High Assurance Computing Systems (8/5/93). (Atkinson NRL, KX Records)				
	C1004	Henning Schulzrinne, <i>Personal Mobility For Multimedia Services In The Internet</i> , Proceedings of the Interactive Distributed Multimedia Systems and Services European Workshop at 143 (1996). (Schulzrinne 96)				
	C1005	Microsoft Corp., <i>Microsoft Virtual Private Networking: Using Point-to-Point Tunneling Protocol for Low-Cost, Secure, Remote Access Across the Internet</i> (1996) (printed from 1998 PDC DVD-ROM). (Point to Point, Microsoft Prior Art VPN Technology)				
	C1006	"Safe Surfing: How to Build a Secure World Wide Web Connection," IBM Technical Support Organization, (March 1996). (Safe Surfing, WEBSITE ART)				
	C1007	Goldschlag, et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK (May 1996). (Goldschlag II, Onion Routing)				
	C1008	"IPSec Minutes From Montreal", IPSEC Working Group Meeting Notes, http://www.sandleman.ca/ipsec/1996/08/msg00018.html (June 1996) (IPSec Minutes, FreeSWAN)				
	C1009	J M Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California, July 1996. (Galvin, DNSSEC)				
	C1010	J Gilmore, et al. "Re: Key Management, anyone? (DNS Keying)," IPSec Working Group Mailing List Archives (8/96). (Gilmore DNS, FreeSWAN)				
	C1011	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, FreeSWAN)				
	C1012	Arnt Gulbrandsen & Paul Vixie, <i>A DNS RR for specifying the location of services (DNS SRV)</i> , IETF RFC 2052 (October 1996). (RFC 2052, DNS SRV)				
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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known		
				Application Number	11/839,987	
				Filing Date	August 16, 2007	
				First Named Inventor	Edmund Colby Munger	
				Art Unit	2453	
				Examiner Name	Lim, Krisna	
Sheet	3	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)	
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				
	C1013	Freier, et al "The SSL Protocol Version 3.0," Transport Layer Security Working Group (November 18, 1996). (SSL, UNDERLYING SECURITY TECHNOLOGY)				
	C1014	M. Handley, H Schulzrinne, E Schooler, Internet Engineering Task Force, Internet Draft, (12/02/1996). (RFC 2543 Internet Draft 1) [Due to difficulty locating this reference, a copy has not been provided]				
	C1015	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)				
	C1016	Kenneth F Alden & Edward P. Wobber, <i>The AltaVista Tunnel: Using the Internet to Extend Corporate Networks</i> , Digital Technical Journal (1997) (Alden, AltaVista)				
	C1017	Automotive Industry Action Group, "ANX Release 1 Document Publication," AIAG (1997). (AIAG, ANX)				
	C1018	Automotive Industry Action Group, "ANX Release 1 Draft Document Publication," AIAG Publications (1997). (AIAG Release, ANX)				
	C1019	Aventail Corp., "AutoSOCKS v 2.1 Datasheet," available at http://www.archive.org/web/19970212013409/www.aventail.com/prod/autosk2ds.html (1997). (AutoSOCKS, Aventail) [Due to difficulty locating this reference, a copy has not been provided]				
	C1020	Aventail Corp. "Aventail VPN Data Sheet," available at http://www.archive.org/web/19970212013043/www.aventail.com/prod/vpndata.html (1997). (Data Sheet, Aventail)				
	C1021	Aventail Corp., "Directed VPN Vs. Tunnel," available at http://web.archive.org/web/19970620030312/www.aventail.com/educate/directvpn.html (1997). (Directed VPN, Aventail)				
	C1022	Aventail Corp., "Managing Corporate Access to the Internet," Aventail AutoSOCKS White Paper available at http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/ipmwp.html (1997). (Corporate Access, Aventail)				
	C1023	Aventail Corp., "Socks Version 5," Aventail Whitepaper, available at http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/sockswp.html (1997). (Socks, Aventail) [Due to difficulty locating this reference, a copy has not been provided]				
	C1024	Aventail Corp., "VPN Server V2.0 Administration Guide," (1997) (VPN, Aventail)				
	C1025	Goldschlag, et al " <i>Privacy on the Internet</i> ," Naval Research Laboratory, Center for High Assurance Computer Systems (1997). (Goldschlag I, Onion Routing)				
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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known		
				Application Number	11/839,987	
				Filing Date	August 16, 2007	
				First Named Inventor	Edmund Colby Munger	
				Art Unit	2453	
				Examiner Name	Lim, Krisna	
Sheet	4	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)	
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.				
	C1026	Microsoft Corp., <i>Installing Configuring and Using PPTP with Microsoft Clients and Servers</i> (1997). (Using PPTP, Microsoft Prior Art VPN Technology)				
	C1027	Microsoft Corp., <i>IP Security for Microsoft Windows NT Server 5.0</i> (1997) (printed from 1998 PDC DVD-ROM). (IP Security, Microsoft Prior Art VPN Technology)				
	C1028	Microsoft Corp., <i>Microsoft Windows NT Active Directory: An Introduction to the Next Generation Directory Services</i> (1997) (printed from 1998 PDC DVD-ROM) (Directory, Microsoft Prior Art VPN Technology)				
	C1029	Microsoft Corp., <i>Routing and Remote Access Service for Windows NT Server New Opportunities Today and Looking Ahead</i> (1997) (printed from 1998 PDC DVD-ROM). (Routing, Microsoft Prior Art VPN Technology)				
	C1030	Microsoft Corp., <i>Understanding Point-to-Point Tunneling Protocol PPTP</i> (1997) (printed from 1998 PDC DVD-ROM). (Understanding PPTP, Microsoft Prior Art VPN Technology)				
	C1031	J Mark Smith et al., <i>Protecting a Private Network: The AltaVista Firewall</i> , Digital Technical Journal (1997). (Smith, AltaVista)				
	C1032	Naganand Doraswamy <i>Implementation of Virtual Private Networks (VPNs) with IP Security</i> , <draft-ietf-ipsec-vpn-00.txt> (March 12, 1997). (Doraswamy)				
	C1033	M Handley, H Schulzrinne, E Schooler, Internet Engineering Task Force, Internet Draft, (03/27/1997). (RFC 2543 Internet Draft 2) [Due to difficulty locating this reference, a copy has not been provided]				
	C1034	Aventail Corp., "Aventail and Cybersafe to Provide Secure Authentication For Internet and Intranet Communication," Press Release, April 3, 1997. (Secure Authentication, Aventail)				
	C1035	D Wagner, et al. "Analysis of the SSL 3.0 Protocol," (April 15, 1997) (Analysis, UNDERLYING SECURITY TECHNOLOGIES)				
	C1036	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)				
	C1037	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)				
	C1038	Aventail Corp., "Aventail Announces the First VPN Solution to Assure Interoperability Across Emerging Security Protocols," June 2, 1997. (First VPN, Aventail)				
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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known		
				Application Number	11/839,987	
				Filing Date	August 16, 2007	
				First Named Inventor	Edmund Colby Munger	
				Art Unit	2453	
Examiner Name	Lim, Krisna					
Sheet	5	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)	
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				
	C1039	Syverson, et al. "Private Web Browsing," Naval Research Laboratory, Center for High 8 Assurance Computer Systems (June 2, 1997). (Syverson, Onion Routing)				
	C1040	Bellcore, "Metrics, Criteria, and Measurement Technique Requirements for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (June 16, 1997) (AIAG Requirements, ANX)				
	C1041	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/31/1997). (RFC 2543 Internet Draft 3) [Due to difficulty locating this reference, a copy has not been provided]				
	C1042	R. Atkinson, "Key Exchange Delegation Record for the DNS," Network Working Group, RFC 2230 (November 1997). (RFC 2230, KX Records)				
	C1043	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/11/1997). (RFC 2543 Internet Draft 4) [Due to difficulty locating this reference, a copy has not been provided]				
	C1044	1998 Microsoft Professional Developers Conference DVD ("1998 PDC DVD-ROM") (including screenshots captured therefrom and produced as MSFTVX 00018827-00018832). (Conference, Microsoft Prior Art VPN Technology)				
	C1045	Microsoft Corp., <i>Virtual Private Networking An Overview</i> (1998) (printed from 1998 PDC DVD-ROM) (Overview, Microsoft Prior Art VPN Technology)				
	C1046	Microsoft Corp., <i>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</i> (1998) (available at hap //www.microsoft.com/presspass/features/1998/10-19nt5.mspxptrue). (NT Beta, Microsoft Prior Art VPN Technology)				
	C1047	"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)				
	C1048	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)				
	C1049	R. G. Moskowitz, "Network Address Translation Issues with IPsec," Internet Draft, Internet Engineering Task Force, February 6, 1998. (Moskowitz)				
	C1050	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)				
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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	11/839,987
				Filing Date	August 16, 2007
				First Named Inventor	Edmund Colby Munger
				Art Unit	2453
Examiner Name	Lim, Krisna				
Sheet	6	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)
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			
	C1051	C. Huitema, 45 al "Simple Gateway Control Protocol," Version 1 0 (May 5, 1998) (SGCP)			
	C1052	DISA "Secret Internet Protocol Router Network," SIPRNET Program Management Office (D3113) DISN Networks, DISN Transmission Services (May 8, 1998). (DISA, SIPRNET)			
	C1053	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (05/14/1998) (RFC 2543 Internet Draft 5) [Due to difficulty locating this reference, a copy has not been provided]			
	C1054	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (06/17/1998) (RFC 2543 Internet Draft 6) [Due to difficulty locating this reference, a copy has not been provided]			
	C1055	D. McDonald, et al. "PF_KEY Key Management API, Version 2," Network Working Group, RFC 2367 (July 1998). (RFC 2367)			
	C1056	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/16/1998) (RFC 2543 Internet Draft 7) [Due to difficulty locating this reference, a copy has not been provided]			
	C1057	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (08/07/1998) (RFC 2543 Internet Draft 8) [Due to difficulty locating this reference, a copy has not been provided]			
	C1058	Microsoft Corp., <i>Company Focuses on Quality and Customer Feedback</i> (August 18, 1998). (Focus, Microsoft Prior Art VPN Technology)			
	C1059	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (09/18/1998) (RFC 2543 Internet Draft 9) [Due to difficulty locating this reference, a copy has not been provided]			
	C1060	Atkinson, et al. "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998). (RFC 2401, UNDERLYING SECURITY TECHNOLOGIES)			
	C1061	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/12/1998) (RFC 2543 Internet Draft 10) 9 [Due to difficulty locating this reference, a copy has not been provided]			
	C1062	Donald Eastlake, <i>Domain Name System Security Extensions</i> , IETF DNS Security Working Group (December 1998). (DNSSEC-7)			
	C1063	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/15/1998) (RFC 2543 Internet Draft 11) [Due to difficulty locating this reference, a copy has not been provided]			
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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known		
				Application Number	11/839,987	
				Filing Date	August 16, 2007	
				First Named Inventor	Edmund Colby Munger	
				Art Unit	2453	
Examiner Name	Lim, Krisna					
Sheet	7	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)	
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				
	C1064	Aventail Corp., "Aventail Connect 3 1/2 6 Administrator's Guide," (1999). (Aventail Administrator 3 1, Aventail) [Due to difficulty locating this reference, a copy has not been provided]				
	C1065	Aventail Corp., "Aventail Connect 3 1/2 6 User's Guide," (1999) (Aventail User 3 1, Aventail) [Due to difficulty locating this reference, a copy has not been provided]				
	C1066	Aventail Corp., "Aventail ExtraWeb Server v3 2 Administrator's Guide," (1999) (Aventail ExtraWeb 3 2, Aventail) [Due to difficulty locating this reference, a copy has not been provided]				
	C1067	Kaufman et al, "Implementing IPsec," (Copyright 1999). (Implementing IPSEC, VPN REFERENCES)				
	C1068	Network Solutions, Inc. "Enabling SSL," NSI Registry (1999). (Enabling SSL, UNDERLYING SECURITY TECHNOLOGIES)				
	C1069	Check Point Software Technologies Ltd (1999) (Check Point, Checkpoint FW) [Due to difficulty locating this reference, a copy has not been provided]				
	C1070	Arnt Gulbrandsen & Paul Vixie, <i>A DNS RR for specifying the location of services (DNS SRV)</i> , <draft-ietf-dnsind-frc2052bis-02.txt> (January 1999). (Gulbrandsen 99, DNS SRV)				
	C1071	C. Scott, et al <i>Virtual Private Networks</i> , O'Reilly and Associates, Inc., 2nd ed (Jan. 1999). (Scott VPNs)				
	C1072	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (01/15/1999) (RFC 2543 Internet Draft 12) [Due to difficulty locating this reference, a copy has not been provided]				
	C1073	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)				
	C1074	H. Schulzrinne, "Internet Telephony: architecture and protocols – an IETF perspective," Computer Networks, Vol. 31, No. 3 (February 1999). (Telephony, Schulzrinne)				
	C1075	M. Handley, et al. "SIP: Session Initiation Protocol," Network Working Group, RFC 2543 and Internet Drafts (12/96-3/99). (Handley, RFC 2543)				
	C1076	FreeSWAN Project, <i>Linux FreeSWAN Compatibility Guide</i> (March 4, 1999). (FreeSWAN Compatibility Guide, FreeSWAN)				
	C1077	Telcordia Technologies, "ANX Release 1 Document Corrections," AIAG (May 11, 1999). (Telcordia, ANX)				
	C1078	Ken Hornstein & Jeffrey Altman, <i>Distributing Kerberos KDC and Realm Information with DNS</i> <draft-eitf-cat-krb-dns-locate-oo.txt> (June 21, 1999). (Hornstein, DNS SRV)				
EXAMINER				DATE CONSIDERED		

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609 Draw line through citation if not in conformance and not considered Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional) 2 Applicant is to place a check mark here if English language Translation is attached

Subst. for form 1449/PTO				Complete if Known	
SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Application Number	11/839,987
				Filing Date	August 16, 2007
				First Named Inventor	Edmund Colby Munger
				Art Unit	2453
				Examiner Name	Lim, Krisna
Sheet	8	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)
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			
	C1079	Bhattacharya et. al. "An LDAP Schema for Configuration and Administration of IPsec Based Virtual Private Networks (VPNs)", IETF Internet Draft (October 1999) (Bhattacharya LDAP VPN)			
	C1080	B. Patel, et al. "DHCP Configuration of IPSEC Tunnel Mode," IPSEC Working Group, Internet Draft 02 (10/15/1999). (Patel)			
	C1081	Goncalves, et al. <i>Check Point FireWall -1 Administration Guide</i> , McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW) [Due to difficulty locating this reference, a copy has not been provided]			
	C1082	"Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources," FirstVPN, (Jan 2000). (FirstVPN Microsoft)			
	C1083	Gulbrandsen, Vixie, & Esibov, <i>A DNS RR for specifying the location of services (DNS SRV)</i> , IETF RFC 2782 (February 2000). (RFC 2782, DNS SRV)			
	C1084	MITRE Organization, "Technical Description," Collaborative Operations in Joint Expeditionary Force Experiment (JEFX) 99 (February 2000). (MITRE, SIPRNET)			
	C1085	H Schulzrinne, et al. "Application-Layer Mobility Using SIP," <i>Mobile Computing and Communications Review</i> , Vol. 4, No. 3. pp. 47-57 (July 2000). (Application, SIP)			
	C1086	Kindred et al, "Dynamic VPN Communities: Implementation and Experience," DARPA Information Survivability Conference and Exposition II (June 2001) (DARPA, VPN SYSTEMS)			
	C1087	ANX 101: Basic ANX Service Outline. (Outline, ANX)			
	C1088	ANX 201: Advanced ANX Service. (Advanced, ANX)			
	C1089	Appendix A: Certificate Profile for ANX IPsec Certificates. (Appendix, ANX)			
	C1090	Assured Digital Products. (Assured Digital) [Due to difficulty locating this reference, a copy has not been provided]			
	C1091	Aventail Corp., "Aventail AutoSOCKS the Client Key to Network Security," Aventail Corporation White Paper. (Network Security, Aventail)			
	C1092	Cindy Moran, "DISN Data Networks: Secret Internet Protocol Router Network (SIPRNet)." (Moran, SIPRNET)			
	C1093	Data Fellows F-Secure VPN+ (F-Secure VPN+)			
	C1094	"Interim Operational Systems Doctrine for the Remote Access Security Program (RASP) Secret Dial-In Solution. (RASP, SIPRNET)			
	C1095	<i>Onion Routing</i> , "Investigation of Route Selection Algorithms," available at http://www.onion-router.net/Archives/Route/index.html . (Route Selection, Onion Routing)			
	C1096	Secure Computing, "Bullet-Proofing an Army Net," Washington Technology (Secure, SIPRNET)			
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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known		
				Application Number	11/839,987	
				Filing Date	August 16, 2007	
				First Named Inventor	Edmund Colby Munger	
				Art Unit	2453	
				Examiner Name	Lim, Krisna	
Sheet	9	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)	
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				
	C1097	SPARTA "Dynamic Virtual Private Network" (Sparta, VPN SYSTEMS)				
	C1098	Standard Operation Procedure for Using the 1910 Secure Modems. (Standard, SIPRNET)				
	C1099	Publicly available emails relating to FreeS/WAN (MSFTVX00018833-MSFTVX00019206). (FreeS/WAN emails, FreeS/WAN)				
	C1100	Kaufman et al, "Implementing IPsec," (Copyright 1999) (Implementing IPsec)				
	C1101	Network Associates <i>Gauntlet Firewall For Unix User's Guide Version 5.0</i> (1999). (Gauntlet User's Guide - Unix, Firewall Products)				
	C1102	Network Associates <i>Gauntlet Firewall For Windows NT Getting Started Guide Version 5.0</i> (1999) (Gauntlet Getting Started Guide - NT, Firewall Products)				
	C1103	Network Associates <i>Gauntlet Firewall For Unix Getting Started Guide Version 5.0</i> (1999) (Gauntlet Unix Getting Started Guide, Firewall Products)				
	C1104	Network Associates <i>Release Notes Gauntlet Firewall for Unix 5.0</i> (March 19, 1999) (Gauntlet Unix Release Notes, Firewall Products)				
	C1105	Network Associates <i>Gauntlet Firewall For Windows NT Administrator's Guide Version 5.0</i> (1999) (Gauntlet NT Administrator's Guide, Firewall Products)				
	C1106	Trusted Information Systems, Inc <i>Gauntlet Internet Firewall Firewall-to-Firewall Encryption Guide Version 3.1</i> (1996) (Gauntlet Firewall-to-Firewall, Firewall Products)				
	C1107	Network Associates <i>Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0</i> (1999) (Gauntlet NT GVPN, GVPN)				
	C1108	Network Associates <i>Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0</i> (1999) (Gauntlet Unix GVPN, GVPN)				
	C1109	Dan Sterne <i>Dynamic Virtual Private Networks</i> (May 23, 2000) (Sterne DVPN, DVPN)				
	C1110	Darrell Kindred <i>Dynamic Virtual Private Networks (DVPN)</i> (December 21, 1999) (Kindred DVPN, DVPN)				
	C1111	Dan Sterne <i>et al. TIS Dynamic Security Perimeter Research Project Demonstration</i> (March 9, 1998) (Dynamic Security Perimeter, DVPN)				
	C1112	Darrell Kindred <i>Dynamic Virtual Private Networks Capability Description</i> (January 5, 2000) (Kindred DVPN Capability, DVPN) 11				
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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	11/839,987
				Filing Date	August 16, 2007
				First Named Inventor	Edmund Colby Munger
				Art Unit	2453
Examiner Name	Lim, Krisna				
Sheet	10	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)
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.			
	C1113	October 7, and 28 1997 email from Domenic J. Turchi Jr (SPARTA00001712-1714, 1808-1811) (Turchi DVPN email, DVPN)			
	C1114	James Just & Dan Sterne <i>Security Quickstart Task Update</i> (February 5, 1997) (Security Quickstart, DVPN)			
	C1115	Virtual Private Network Demonstration dated March 21, 1998 (SPARTA00001844-54) (DVPN Demonstration, DVPN)			
	C1116	GTE Internetworking & BBN Technologies <i>DARPA Information Assurance Program Integrated Feasibility Demonstration (IFD) 1.1 Plan</i> (March 10, 1998) (IFD 1.1, DVPN)			
	C1117	Microsoft Corp Windows NT Server Product Documentation: Administration Guide – Connection Point Services, <i>available at</i> 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.)			
	C1118	Microsoft Corp. Windows NT Server Product Documentation: Administration Kit Guide – Connection Manager, <i>available at</i> 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.)			
	C1119	Microsoft Corp. Autodial Heuristics, <i>available at</i> 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.)			
	C1120	Microsoft Corp., Cariplo: Distributed Component Object Model, (1996) <i>available at</i> http://msdn2.microsoft.com/en-us/library/ms809332(printer).aspx (Cariplo I)			
	C1121	Marc Levy, COM Internet Services (Apr. 23, 1999), <i>available at</i> http://msdn2.microsoft.com/en-us/library/ms809302(printer).aspx (Levy)			
	C1122	Markus Horstmann and Mary Kirtland, DCOM Architecture (July 23, 1997), <i>available at</i> http://msdn2.microsoft.com/en-us/library/ms809311(printer).aspx (Horstmann)			
	C1123	Microsoft Corp., DCOM: A Business Overview (Apr. 1997), <i>available at</i> http://msdn2.microsoft.com/en-us/library/ms809320(printer).aspx (DCOM Business Overview I)			
	C1124	Microsoft Corp., DCOM Technical Overview (Nov. 1996), <i>available at</i> http://msdn2.microsoft.com/en-us/library/ms809340(printer).aspx (DCOM Technical Overview I)			
	C1125	Microsoft Corp., DCOM Architecture White Paper (1998) <i>available in</i> PDC DVD-ROM (DCOM Architecture)			
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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known		
				Application Number	11/839,987	
				Filing Date	August 16, 2007	
				First Named Inventor	Edmund Colby Munger	
				Art Unit	2453	
Examiner Name	Lim, Krisna					
Sheet	11	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)	
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				
	C1126	Microsoft Corp, DCOM – The Distributed Component Object Model, A Business Overview White Paper (Microsoft 1997) available in PDC DVD-ROM (DCOM Business Overview II)				
	C1127	Microsoft Corp, DCOM—Cariplo Home Banking Over The Internet White Paper (Microsoft 1996) available in PDC DVD-ROM (Cariplo II)				
	C1128	Microsoft Corp, DCOM Solutions in Action White Paper (Microsoft 1996) available in PDC DVD-ROM (DCOM Solutions in Action)				
	C1129	Microsoft Corp., DCOM Technical Overview White Paper (Microsoft 1996) available 12 in PDC DVD-ROM (DCOM Technical Overview II)				
	C1130	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)				
	C1131	126. Aaron Skonnard, <i>Essential Wininet</i> 313-423 (Addison Wesley Longman 1998) (Essential Wininet)				
	C1132	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)				
	C1133	Microsoft Corp., Internet Connection Services for MS RAS, Standard Edition, http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstart msp x (Internet Connection Services I)				
	C1134	Microsoft Corp., Internet Connection Services for RAS, Commercial Edition, available at http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstrtc msp x (Internet Connection Services II)				
	C1135	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 msp x (IE5 Corporate Development)				
	C1136	Mark Minasi, <i>Mastering Windows NT Server 4</i> 1359-1442 (6th ed, January 15, 1999)(Mastering Windows NT Server)				
	C1137	<i>Hands On, Self-Paced Training for Supporting Version 4.0</i> 371-473 (Microsoft Press 1998) (Hands On)				
	C1138	Microsoft Corp., MS Point-to-Point Tunneling Protocol (Windows NT 4.0), available at http://www.microsoft.com/technet/archive/winntas/maintain/featusability/pptpwp3.msp x (MS PPTP)				
	C1139	Kenneth Gregg, et al, <i>Microsoft Windows NT Server Administrator's Bible</i> 173-206, 883-911, 974-1076 (IDG Books Worldwide 1999) (Gregg)				
	C1140	Microsoft Corp., Remote Access (Windows), available at http://msdn2.microsoft.com/en-us/library/bb545687(VS.85,printer).aspx (Remote Access)				
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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	11/839,987
				Filing Date	August 16, 2007
				First Named Inventor	Edmund Colby Munger
				Art Unit	2453
Examiner Name	Lim, Krisna				
Sheet	12	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)
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			
	C1141	Microsoft Corp., Understanding PPTP (Windows NT 4.0), available at http://www.microsoft.com/technet/archive/winntas/plan/pptpudst.msp (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.)			
	C1142	Microsoft Corp., Windows NT 4.0: Virtual Private Networking, available at http://www.microsoft.com/technet/archive/winntas/deploy/confeat/vpntwk.msp (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.)			
	C1143	Anthony Northrup, <i>NT Network Plumbing: Routers, Proxies, and Web Services</i> 299-399 (IDG Books Worldwide 1998) (Network Plumbing)			
	C1144	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/rrasch01.msp (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			
	C1145	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.msp (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.)			
	C1146	F-Secure, <i>F-Secure Evaluation Kit</i> (May 1999) (FSECURE 00000003) (Evaluation Kit 3) [Due to difficulty locating this reference, a copy has not been provided]			
	C1147	F-Secure, <i>F-Secure NameSurfer</i> (May 1999) (from FSECURE 00000003) (NameSurfer 3)			
	C1148	F-Secure, <i>F-Secure VPN Administrator's Guide</i> (May 1999) (from FSECURE 00000003) (F-Secure VPN 3)			
	C1149	F-Secure, <i>F-Secure SSH User's & Administrator's Guide</i> (May 1999) (from FSECURE 00000003) (SSH Guide 3)			
	C1150	F-Secure, <i>F-Secure SSH2.0 for Windows NT and 95</i> (May 1999) (from FSECURE 00000003) (SSH 2.0 Guide 3)			
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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known		
				Application Number	11/839,987	
				Filing Date	August 16, 2007	
				First Named Inventor	Edmund Colby Munger	
				Art Unit	2453	
				Examiner Name	Lim, Krisna	
Sheet	13	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)	
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				
	C1151	F-Secure, <i>F-Secure VPN+ Administrator's Guide</i> (May 1999) (from FSECURE 00000003) (VPN+ Guide 3)				
	C1152	F-Secure, <i>F-Secure VPN+ 4.1</i> (1999) (from FSECURE 00000006) (VPN+ 4.1 Guide 6)				
	C1153	F-Secure, <i>F-Secure SSH</i> (1996) (from FSECURE 00000006) (F-Secure SSH 6)				
	C1154	F-Secure, <i>F-Secure SSH 2.0 for Windows NT and 95</i> (1998) (from FSECURE 00000006) (F-Secure SSH 2.0 Guide 6)				
	C1155	F-Secure, <i>F-Secure Evaluation Kit</i> (Sept. 1998) (FSECURE 00000009) (Evaluation Kit 9) [Due to difficulty locating this reference, a copy has not been provided]				
	C1156	F-Secure, <i>F-Secure SSH User's & Administrator's Guide</i> (Sept 1998) (from FSECURE 00000009) (SSH Guide 9)				
	C1157	F-Secure, <i>F-Secure SSH 2.0 for Windows NT and 95</i> (Sept 1998) (from FSECURE 00000009) (F-Secure SSH 2.0 Guide 9)				
	C1158	F-Secure, <i>F-Secure VPN+</i> (Sept. 1998) (from FSECURE 00000009) (VPN+ Guide 9)				
	C1159	F-Secure, <i>F-Secure Management Tools, Administrator's Guide</i> (1999) (from FSECURE 00000003) (F-Secure Management Tools)				
	C1160	F-Secure, <i>F-Secure Desktop, User's Guide</i> (1997) (from FSECURE 00000009) (FSecure Desktop User's Guide)				
	C1161	SafeNet, Inc, <i>VPN Policy Manager</i> (January 2000) (VPN Policy Manager)				
	C1162	F-Secure, <i>F-Secure VPN+ for Windows NT 4.0</i> (1998) (from FSECURE 00000009) (FSecure VPN+)				
	C1163	IRE, Inc, <i>SafeNet/Soft-PK Version 4</i> (March 28, 2000) (Soft-PK Version 4) [Due to difficulty locating this reference, a copy has not been provided]				
	C1164	IRE/SafeNet Inc, <i>VPN Technologies Overview</i> (March 28, 2000) (Safenet VPN Overview) [Due to difficulty locating this reference, a copy has not been provided]				
	C1165	IRE, Inc, <i>SafeNet / Security Center Technical Reference Addendum</i> (June 22, 1999) (Safenet Addendum)				
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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known		
				Application Number	11/839,987	
				Filing Date	August 16, 2007	
				First Named Inventor	Edmund Colby Munger	
				Art Unit	2453	
				Examiner Name	Lim, Krisna	
Sheet	14	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)	
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				
	C1166	IRE, Inc., <i>System Description for VPN Policy Manager and SafeNet/SoftPK</i> (March 30, 2000) (VPN Policy Manager System Description)				
	C1167	IRE, Inc., <i>About SafeNet / VPN Policy Manager</i> (1999) (About Safenet VPN Policy Manager)				
	C1168	IRE, Inc., <i>SafeNet/VPN Policy Manager Quick Start Guide Version 1</i> (1999) (SafeNet VPN Policy Manager) [Due to difficulty locating this reference, a copy has not been provided]				
	C1169	Trusted Information Systems, Inc., <i>Gauntlet Internet Firewall, Firewall Product Functional Summary</i> (July 22, 1996) (Gauntlet Functional Summary)				
	C1170	Trusted Information Systems, Inc., <i>Running the Gauntlet Internet Firewall, An Administrator's Guide to Gauntlet Version 3.0</i> (May 31, 1995) (Running the Gauntlet Internet Firewall)				
	C1171	Ted Harwood, <i>Windows NT Terminal Server and Citrix Metaframe</i> (New Riders 1999) (Windows NT Harwood) 79				
	C1172	Todd W. Mathers and Shawn P. Genoway, <i>Windows NT Thin Client Solutions: Implementing Terminal Server and Citrix MetaFrame</i> (Macmillan Technial Publishing 1999) (Windows NT Mathers)				
	C1173	Bernard Aboba et al, <i>Securing L2TP using IPSEC</i> (February 2, 1999)				
	C1174	156 <i>Finding Your Way Through the VPN Maze</i> (1999) ("PGP")				
	C1175	Linux FreeSWAN Overview (1999) (Linux FreeSWAN) Overview)				
	C1176	TimeStep, <i>The Business Case for Secure VPNs</i> (1998) ("TimeStep")				
	C1177	WatchGuard Technologies, Inc., <i>WatchGuard Firebox System Powerpoint</i> (2000) [Due to difficulty locating this reference, a copy has not been provided]				
	C1178	WatchGuard Technologies, Inc., <i>MSS Firewall Specifications</i> (1999) [Due to difficulty locating this reference, a copy has not been provided]				
	C1179	WatchGuard Technologies, Inc., <i>Request for Information, Security Services</i> (2000) [Due to difficulty locating this reference, a copy has not been provided]				
	C1180	WatchGuard Technologies, Inc., <i>Protecting the Internet Distributed Enterprise, White Paper</i> (February 2000) [Due to difficulty locating this reference, a copy has not been provided]				
EXAMINER				DATE CONSIDERED		

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 809 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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known		
				Application Number	11/839,987	
				Filing Date	August 16, 2007	
				First Named Inventor	Edmund Colby Munger	
				Art Unit	2453	
				Examiner Name	Lim, Krisna	
Sheet	15	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)	
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.				
	C1181	WatchGuard Technologies, Inc., <i>WatchGuard LiveSecurity for MSS Powerpoint</i> (Feb. 14 2000)				
	C1182	WatchGuard Technologies, Inc., <i>MSS Version 2.5, Add-On for WatchGuard SOHO Releaset Notes</i> (July 21, 2000) [Due to difficulty locating this reference, a copy has not been provided]				
	C1183	Air Force Research Laboratory, <i>Statement of Work for Information Assurance System Architecture and Integration, PR No. N-8-6106 (Contract No F30602-98-C-0012)</i> (January 29, 1998)				
	C1184	GTE Internetworking & BBN Technologies <i>DARPA Information Assurance Program Integrated Feasibility Demonstration (IFD) 1.2 Report, Rev. 1.0</i> (September 21, 1998)				
	C1185	BBN Information Assurance Contract, <i>TIS Labs Monthly Status Report</i> (March 16-April 30, 1998)				
	C1186	DARPA, <i>Dynamic Virtual Private Network (VPN) Powerpoint</i>				
	C1187	GTE Internetworking, <i>Contractor's Program Progress Report</i> (March 16-April 30, 1998)				
	C1188	Darrell Kindred, <i>Dynamic Virtual Private Networks (DVPN) Countermeasure Characterization</i> (January 30, 2001)				
	C1189	<i>Virtual Private Networking Countermeasure Characterization</i> (March 30, 2000)				
	C1190	<i>Virtual Private Network Demonstration</i> (March 21, 1998)				
	C1191	Information Assurance/NAI Labs, <i>Dynamic Virtual Private Networks (VPNs) and Integrated Security Management</i> (2000)				
	C1192	Information Assurance/NAI Labs, <i>Create/Add DVPN Enclave</i> (2000)				
	C1193	NAI Labs, <i>IFE 3.1 Integration Demo</i> (2000)				
	C1194	Information Assurance, <i>Science Fair Agenda</i> (2000)				
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.
 † 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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	11/839,987
				Filing Date	August 16, 2007
				First Named Inventor	Edmund Colby Munger
				Art Unit	2453
				Examiner Name	Lim, Krisna
Sheet	16	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)
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			
	C1195	Darrell Kindred et al , <i>Proposed Threads for IFE 3 1</i> (January 13, 2000)			
	C1196	<i>IFE 3 1 Technology Dependencies</i> (2000)			
	C1197	<i>IFE 3 1 Topology</i> (February 9, 2000)			
	C1198	Information Assurance, <i>Information Assurance Integration: IFE 3.1, Hypothesis & Thread Development</i> (January 10-11, 2000)			
	C1199	Information Assurance/NAI Labs, <i>Dynamic Virtual Private Networks Presentation</i> (2000)			
	C1200	Information Assurance/NAI Labs, <i>Dynamic Virtual Private Networks Presentation v. 2</i> (2000)			
	C1201	Information Assurance/NAI Labs, <i>Dynamic Virtual Private Networks Presentation v. 3</i> (2000) [Due to difficulty locating this reference, a copy has not been provided]			
	C1202	T. Braun et al , <i>Virtual Private Network Architecture, Charging and Accounting Technology for the Internet</i> (August 1, 1999) (VPNA)			
	C1203	Network Associates Products – <i>PGP Total Network Security Suite, Dynamic Virtual Private Networks</i> (1999)			
	C1204	Microsoft Corporation, <i>Microsoft Proxy Server 2 0</i> (1997) (Proxy Server 2.0, Microsoft Prior Art VPN Technology)			
	C1205	David Johnson et. al , <i>A Guide To Microsoft Proxy Server 2 0</i> (1999) (Johnson, Microsoft Prior Art VPN Technology)			
	C1206	Microsoft Corporation, <i>Setting Server Parameters</i> (1997 (copied from Proxy Server 2 0 CD labeled MSFTVX00157288) (Setting Server Parameters, Microsoft Prior Art VPN Technology)			
	C1207	Kevin Schuler, <i>Microsoft Proxy Server 2</i> (1998) (Schuler, Microsoft Prior Art VPN Technology)			
	C1208	Erik Rozell et al , <i>MCSE Proxy Server 2 Study Guide</i> (1998) (Rozell, Microsoft Prior 15 Art VPN Technology)			
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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Complete if Known	
				Application Number	11/839,987
				Filing Date	August 16, 2007
				First Named Inventor	Edmund Colby Munger
				Art Unit	2453
				Examiner Name	Lim, Krisna
Sheet	17	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)
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.			
	C1209	M Shane Stigler & Mark A Linsenhardt, <i>IIS 4 and Proxy Server 2</i> (1999) (Stigler, Microsoft Prior Art VPN Technology)			
	C1210	David G Schaer, <i>MCSE Test Success: Proxy Server 2</i> (1998) (Schaer, Microsoft Prior Art VPN Technology)			
	C1211	John Savill, <i>The Windows NT and Windows 2000 Answer Book</i> (1999) (Savill, Microsoft Prior Art VPN Technology)			
	C1212	Network Associates <i>Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0</i> (1999) (Gauntlet NT GVPN, GVPN)			
	C1213	Network Associates <i>Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0</i> (1999) (Gauntlet Unix GVPN, GVPN)			
	C1214	File History for U S Application Serial No. 09/653,201, Applicant(s): Whittle Bryan, et al , Filing Date 08/31/2000.			
	C1215	<i>AutoSOCKS v2.1</i> , Datasheet, http://web.archive.org/web/19970212013409/www.aventail.com/prod/autoskds.html			
	C1216	Ran Atkinson, <i>Use of DNS to Distribute Keys</i> , 7 Sept 1993, http://ops.ietf.org/lists/namedroppers/namedroppers.199x/msg00945.html			
	C1217	FirstVPN Enterprise Networks, Overview			
	C1218	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			
	C1219	The TLS Protocol Version 1.0; January 1999; page 65 of 71			
	C1220	Elizabeth D. Zwicky, et al , <i>Building Internet Firewalls</i> , 2nd Ed.			
	C1221	Virtual Private Networks – Assured Digital Incorporated – ADI 4500; http://web.archive.org/web/19990224050035/www.assured-digital.com/products/prodvpn/adia4500.htm			
	C1222	Accessware – The Third Wave in Network Security, Conclave from Internet Dynamics; http://web.archive.org/web/11980210013830/interdyn.com/Accessware.html			
	C1223	Extended System Press Release, Sept 2, 1997; <i>Extended VPN Uses The Internet to Create Virtual Private Networks</i> , www.extendedsystems.com			
	C1224	Socks Version 5; Executive Summary; http://web.archive.org/web/199970620031945/www.aventail.com/educate/whitepaper/socks/wp.html			
	C1225	Internet Dynamics First to Ship Integrated Security Solutions for Enterprise Intranets and Extranets; Sept. 15, 1997; http://web.archive.org/web/19980210014150/interdyn.com			
	C1226	Emails from various individuals to Linux IPsec re: DNS-LDAP Splicing			
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

BS199 1623736-1 077580 0066

Electronic Patent Application Fee Transmittal

Application Number:	11839987
Filing Date:	16-Aug-2007
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Atabak R Royae/Jacqueline Andreu
Attorney Docket Number:	77580-0066 (VRNK-1 CP2DVCN)

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
Total in USD (\$)				180

Electronic Acknowledgement Receipt

EFS ID:	5654790
Application Number:	11839987
International Application Number:	
Confirmation Number:	9470
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Atabak R Royae/Jacqueline Andreu
Filer Authorized By:	Atabak R Royae
Attorney Docket Number:	77580-0066 (VRNK-1CP2DVCN)
Receipt Date:	07-JUL-2009
Filing Date:	16-AUG-2007
Time Stamp:	13:45:07
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$180
RAM confirmation Number	9
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 1.21 (Miscellaneous fees and charges)

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	Statement.pdf	91982 d9232e64bfbee1d31269a14ca1ff32968d84cd8	no	2
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Filed (SB/08)	IDS.pdf	1833096 e806ef99db1e902c5ac7c88f933abf8e441245b7	no	17
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Fee Worksheet (PTO-875)	fee-info.pdf	30757 26d58ddc68588641ca35f10623b6064a2d89f4b2	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			1955835		
<p>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.</p> <p><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.</p> <p><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.</p> <p><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.</p>					

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

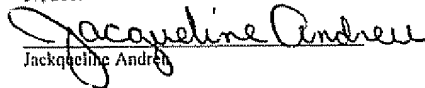
Applicant : Munger et al.
Appl. No. : 11/839,987

Customer No.: 23,630
Confirmation No.: 9470

Filed : August 16, 2007

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this correspondence is being electronically-
transmitted to the United States Patent and Trademark Office on July
07, 2009


Jacqueline Andrew

Title : METHOD FOR ESTABLISHING
SECURE COMMUNICATION LINK
BETWEEN COMPUTERS OF
VIRTUAL PRIVATE NETWORK

Grp./A.U. : 2453
Examiner: : LIM, Krisna

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

INFORMATION DISCLOSURE STATEMENT UNDER 37 C.F.R. § 1.97(b)

Sir:

In accordance with the provisions of 37 C.F.R. 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the documents listed on the attached form PTO-1449. It is respectfully requested that the documents be expressly considered during the prosecution of this application, and that the documents be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement is being filed after the receipt of a First Office Action on the merits for above-referenced application; therefore, a fee \$180.00 is believed to be due with the filing of this paper.

References B1000-B1002 and C998-C1226 were cited by or submitted to the U.S. Patent and Trademark Office in parent application No. 11/679,416, filed Feb. 27, 2007, which is relied

upon for an earlier filing date under 35 USC 120 (the above-identified application is a continuation of application No. 11/679,416). In accordance with 37 C.F.R. § 1.98(d), copies of these references are not attached. Applicants will be pleased to provide copies of the references if requested by the Examiner. The Examiner is invited to contact the undersign agent for any questions and/or copies of references.


This Statement is not to be interpreted as a representation that the cited publications are material, that an exhaustive search has been conducted, or that no other relevant information exists. Nor shall the citation of any publication herein be construed *per se* as a representation that such publication is prior art. Moreover, the Applicant understands that the Examiner will make an independent evaluation of the cited publications.

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

Dated: July 7, 2009

By: 
Atabak R. Royae
Reg. No. 59,037
McDERMOTT, WILL & EMERY, LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4108
Fax (617) 535-3800

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Munger et al.

Customer No.: 23,630

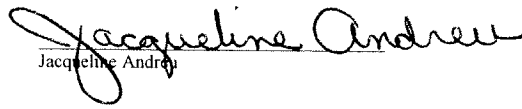
Appl. No. : 11/839,987

Confirmation No.: 9470

Filed : August 16, 2007

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this correspondence is being electronically-transmitted to the United States Patent and Trademark Office on September 21, 2009.


Jacqueline Andrew

Title : METHOD FOR ESTABLISHING
SECURE COMMUNICATION LINK
BETWEEN COMPUTERS OF
VIRTUAL PRIVATE NETWORK

Grp./A.U. : 2453

Examiner: : LIM, Krisna

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

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT
UNDER 37 C.F.R. § 1.97(b)

Sir:

In accordance with the provisions of 37 C.F.R. 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the documents listed on the attached form PTO-1449. It is respectfully requested that the documents be expressly considered during the prosecution of this application, and that the documents be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Supplemental Information Disclosure Statement is being filed after the receipt of a First Office Action on the merits for above-referenced application; therefore, a fee \$180.00 is believed to be due with the filing of this paper.

The 27 references listed in the attached form PTO-1449 were submitted to the U.S. Patent and Trademark Office on September 8, 2009, in parent application No. 11/679,416, filed Feb. 27, 2007, which is relied upon for an earlier filing date under 35 USC 120 (the above-identified application is a continuation of application No. 11/679,416). In accordance with 37 C.F.R. § 1.98(d), copies of these references are not attached. Applicants will be pleased to provide copies of the references if requested by the Examiner. The Examiner is invited to contact the undersign agent for any questions and/or copies of references.

This Statement is not to be interpreted as a representation that the cited publications are material, that an exhaustive search has been conducted, or that no other relevant information exists. Nor shall the citation of any publication herein be construed *per se* as a representation that such publication is prior art. Moreover, the Applicant understands that the Examiner will make an independent evaluation of the cited publications.

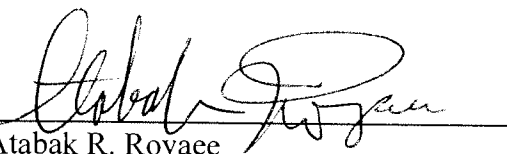
Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-1133 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT, WILL & EMERY, LLP

Dated: September 21, 2009

By:



Atabak R. Royace

Reg. No. 59,037

McDERMOTT, WILL & EMERY, LLP

28 State Street

Boston, MA 02109

Tel. (617) 535-4108

Fax (617) 535-3800

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Subst. for form 1449/PTO		Complete if Known	
				Application Number		11/839,987	
				Filing Date		August 16, 2007	
				First Named Inventor		Victor Larson	
				Art Unit		2453	
Examiner Name		Lim, Krisna					
Sheet	1	of	2	Docket Number	77580-0066 (VRNK-1CP2DVCN2)		

U.S. PATENT DOCUMENTS					
EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code ² (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS							
EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes -Number 4 -Kind Codes (if known)	Publication Date MM-DD-YYYY	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.	
	C1002	DNS-related correspondence dated September 7, 1993 to September 20, 1993. (Pre KX, KX Records)	
	C1014	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/02/1996). (RFC 2543 Internet Draft 1)	
	C1019	Aventail Corp., "AutoSOCKS v. 2.1 Datasheet," available at http://www.archive.org/web/19970212013409/www.aventail.com/prod/autosk2ds.html (1997). (AutoSOCKS, Aventail)	
	C1023	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)	
	C1033	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (03/27/1997). (RFC 2543 Internet Draft 2)	
	C1041	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/31/1997). (RFC 2543 Internet Draft 3)	
	C1043	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/11/1997). (RFC 2543 Internet Draft 4)	
	C1053	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (05/14/1998). (RFC 2543 Internet Draft 5)	
	C1054	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (06/17/1998). (RFC 2543 Internet Draft 6)	
	C1056	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/16/1998). (RFC 2543 Internet Draft 7)	
	C1057	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (08/07/1998). (RFC 2543 Internet Draft 8)	
	C1059	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (09/18/1998). (RFC 2543 Internet Draft 9)	

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.

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Subst. for form 1449/PTO		Complete if Known	
				Application Number		11/839,987	
				Filing Date		August 16, 2007	
				First Named Inventor		Victor Larson	
				Art Unit		2453	
Examiner Name		Lim, Krisna					
Sheet	2	of	2	Docket Number	77580-0066 (VRNK-1CP2DVCN2)		

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.
	C1061	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/12/1998). (RFC 2543 Internet Draft 10)
	C1063	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/15/1998). (RFC 2543 Internet Draft 11)
	C1064	Aventail Corp., "Aventail Connect 3.1/2.6 Administrator's Guide," (1999). (Aventail Administrator 3.1, Aventail)
	C1065	Aventail Corp., "Aventail Connect 3.1/2.6 User's Guide," (1999). (Aventail User 3.1, Aventail)
	C1066	Aventail Corp., "Aventail ExtraWeb Server v3.2 Administrator's Guide," (1999). (Aventail ExtraWeb 3.2, Aventail)
	C1069	Check Point Software Technologies Ltd. (1999) (Check Point, Checkpoint FW)
	C1072	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (01/15/1999). (RFC 2543 Internet Draft 12)
	C1081	Goncalves, et al. <i>Check Point FireWall -1 Administration Guide</i> , McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW)
	C1090	Assured Digital Products. (Assured Digital)
	C1146	F-Secure, <i>F-Secure Evaluation Kit</i> (May 1999) (FSECURE 00000003) (Evaluation Kit 3)
	C1155	F-Secure, <i>F-Secure Evaluation Kit</i> (Sept. 1998) (FSECURE 00000009) (Evaluation Kit 9)
	C1163	IRE, Inc., <i>SafeNet/Soft-PK Version 4</i> (March 28, 2000) (Soft-PK Version 4)
	C1164	IRE/SafeNet Inc., <i>VPN Technologies Overview</i> (March 28, 2000) (Safenet VPN Overview)
	C1168	IRE, Inc., <i>SafeNet/VPN Policy Manager Quick Start Guide Version 1</i> (1999) (SafeNet VPN Policy Manager)
	C1201	Information Assurance/NAI Labs, <i>Dynamic Virtual Private Networks Presentation v.3</i> (2000)
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.

BST99 1629426-1.077580.0066

Electronic Patent Application Fee Transmittal

Application Number:	11839987
Filing Date:	16-Aug-2007
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Atabak R Royae/Jacqueline Andreu
Attorney Docket Number:	77580-0066 (VRNK-1 CP2DVCN)

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
Total in USD (\$)				180

Electronic Acknowledgement Receipt

EFS ID:	6109834
Application Number:	11839987
International Application Number:	
Confirmation Number:	9470
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Atabak R Royae/Jacqueline Andreu
Filer Authorized By:	Atabak R Royae
Attorney Docket Number:	77580-0066 (VRNK-1CP2DVCN)
Receipt Date:	21-SEP-2009
Filing Date:	16-AUG-2007
Time Stamp:	14:31:05
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$180
RAM confirmation Number	647
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 1.21 (Miscellaneous fees and charges)

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed (SB/08)	IDS.pdf	243483 7b67ef89c427a0514910d1cf37f02d895af0b4d3	no	4
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
2	Fee Worksheet (PTO-875)	fee-info.pdf	30757 6489ab7fdaed7e5ee52f8756a5035711dd8f5329	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			274240		
<p>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.</p> <p><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.</p> <p><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.</p> <p><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.</p>					

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Munger et al.

Customer No.: 23,630

Appl. No. : 11/839,987

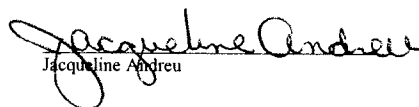
Confirmation No.: 9470

Filed : August 16, 2007

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this correspondence is being electronically-transmitted to the United States Patent and Trademark Office on October 31, 2009.

Title : METHOD FOR ESTABLISHING
SECURE COMMUNICATION LINK
BETWEEN COMPUTERS OF
VIRTUAL PRIVATE NETWORK


Jacqueline Andreu

Grp./A.U. : 2453

Examiner: : LIM, Krisna

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

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT
UNDER 37 C.F.R. § 1.97(b)

Sir:

In accordance with the provisions of 37 C.F.R. 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the documents listed on the attached form PTO-1449. It is respectfully requested that the documents be expressly considered during the prosecution of this application, and that the documents be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Supplemental Information Disclosure Statement is being filed after the receipt of a First Office Action on the merits for above-referenced application; therefore, a fee \$180.00 is believed to be due with the filing of this paper.

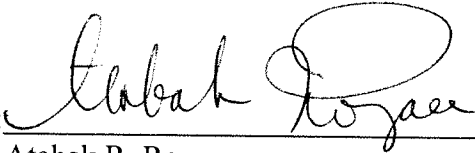
References Nos. C1177-C1180 and C1182 listed in the attached form PTO-1449 were submitted to the U.S. Patent and Trademark Office on October 6, 2009, in parent application No. 11/679,416, filed Feb. 27, 2007, which is relied upon for an earlier filing date under 35 USC 120 (the above-identified application is a continuation of application No. 11/679,416). Also, reference C1181 is being resubmitted because additional pages have been appended to that reference. In accordance with 37 C.F.R. § 1.98(d), copies of these references are not attached. Applicants will be pleased to provide copies of the references if requested by the Examiner. The Examiner is invited to contact the undersign agent for any questions and/or copies of references.

This Statement is not to be interpreted as a representation that the cited publications are material, that an exhaustive search has been conducted, or that no other relevant information exists. Nor shall the citation of any publication herein be construed *per se* as a representation that such publication is prior art. Moreover, the Applicants understand that the Examiner will make an independent evaluation of the cited publications.

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

By: 

Dated: October 31, 2009

Atabak R. Royae
Reg. No. 59,037
McDERMOTT, WILL & EMERY, LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4108
Fax (617) 535-3800

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Subst. for form 1449/PTO		Complete if Known	
				Application Number		11/839,987	
				Filing Date		August 16, 2007	
				First Named Inventor		Victor Larson	
				Art Unit		2453	
Examiner Name		Lim, Krisna					
Sheet	1	of	1	Docket Number	77580-0066 (VRNK-1CP2DVCN2)		

U.S. PATENT DOCUMENTS					
EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code ² (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS							
EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes -Number 4 -Kind Codes (if known)	Publication Date MM-DD-YYYY	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.	
	C1177	WatchGuard Technologies, Inc., <i>WatchGuard Firebox System Powerpoint</i> (2000)	
	C1178	WatchGuard Technologies, Inc., <i>MSS Firewall Specifications</i> (1999)	
	C1179	WatchGuard Technologies, Inc., <i>Request for Information, Security Services</i> (2000)	
	C1180	WatchGuard Technologies, Inc., <i>Protecting the Internet Distributed Enterprise, White Paper</i> (February 2000)	
	C1181	WatchGuard Technologies, Inc., <i>WatchGuard LiveSecurity for MSS Powerpoint</i> (Feb. 14 2000) (resubmitted)	
	C1182	WatchGuard Technologies, Inc., <i>MSS Version 2.5, Add-On for WatchGuard SOHO Release Notes</i> (July 21, 2000)	

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.

Electronic Patent Application Fee Transmittal

Application Number:	11839987			
Filing Date:	16-Aug-2007			
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK			
First Named Inventor/Applicant Name:	Victor Larson			
Filer:	Atabak R Royae/Jacqueline Andreu			
Attorney Docket Number:	77580-0066 (VRNK-1 CP2DVCN)			
Filed as Large Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
Total in USD (\$)				180

Electronic Acknowledgement Receipt

EFS ID:	6369669
Application Number:	11839987
International Application Number:	
Confirmation Number:	9470
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Atabak R Royae/Jacqueline Andreu
Filer Authorized By:	Atabak R Royae
Attorney Docket Number:	77580-0066 (VRNK-1CP2DVCN)
Receipt Date:	31-OCT-2009
Filing Date:	16-AUG-2007
Time Stamp:	17:11:17
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$180
RAM confirmation Number	5851
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 1.21 (Miscellaneous fees and charges)

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed (SB/08)	SupplementalIDS.pdf	150094 <small>02471aae720baca42087482bf75cb890d1f8885e</small>	no	3
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
2	Fee Worksheet (PTO-875)	fee-info.pdf	30757 <small>aeb229dee7e6969cb7073cba8d3d9685ced60260</small>	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			180851		
<p>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.</p> <p><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.</p> <p><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.</p> <p><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.</p>					

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Larson et al.
Application Serial No.: 11/839,987
Filing Date: August 16, 2007
Title: METHOD FOR ESTABLISHING SECURE COMMUNICATION
LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE
NETWORK
Examiner: Lim, Krisna
Art Unit: 2453
Confirmation No.: 9470
Atty. Docket No.: 077580-0066 (VRNK-1CP2DVCN2)

I hereby certify that this correspondence is being electronically transmitted to the United States Patent and Trademark Office via ESF-WEB on December 9, 2009.

/Kelly Ciarmataro/
Kelly Ciarmataro

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

RESPONSE/AMENDMENT

In response to the non-final Office Action mailed June 9, 2009 (“the Office Action”), please amend the above-identified application as follows:

Amendments to the Claims, beginning on page 2 of this paper, and
Remarks, beginning on page 4 of this paper.

Amendments to the Claims

The listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1. (Currently Amended) A method of accessing a secure network address, comprising:
 - sending a query message from a first network device to a secure domain service, the query message requesting from the secure domain service a secure network address for a second network device;
 - receiving at the first network device a response message from the secure domain name service containing the secure network address for the second network device; and
 - sending an access request message from the first network device to the secure network address using a virtual private network communication link.
2. (New) The method according to claim 1, further including supporting a plurality of services over the virtual private network communication link.
3. (New) The method according to claim 2, wherein the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or any combination thereof.
4. (New) The method according to claim 3, wherein the plurality of application programs comprises video conferencing, e-mail, a word processing program, telephony or any combination thereof.
5. (New) The method according to claim 2, wherein the plurality of services comprises audio, video, or any combination thereof.
6. (New) The method according to claim 1, wherein the secure network address includes a security feature.
7. (New) The method according to claim 1, wherein the secure network address is encrypted.

8. (New) The method according to claim 7, further including decrypting the encrypted secure network address.
9. (New) The method according to claim 1, further including supporting a unsecure communication link between the first and second network device.
10. (New) The method according to claim 1, wherein the secure network address is an IP address belonging to the second network device.
11. (New) The method according to claim 1, further including automatically initiating the virtual private network communication link after the access request message is received at the second network device.
12. (New) The method according to claim 1, further including using tunneling over the virtual private network communication link.
13. (New) The method according to claim 1, further including using tunnel packeting over the virtual private network communication link.
14. (New) The method according to claim 1, wherein the secure communication link is an authenticated link.
15. (New) The method according to claim 1, further including performing the method of claim 1 with a client computer connected to a communication network.
16. (New) The method according to claim 1, wherein the second network device has an unsecure name.
17. (New) The method according to claim 1, wherein the secure network address is registered with the secure domain service prior to the step of sending a query message to a secure domain service.
18. (New) The method according to claim 1, further including performing the method of claim 1 with a mobile device connected to a communication network through a cellular network.

Remarks

Applicant appreciates the Examiner's examination of the subject application. Claims 1-18 are currently pending. Claim 1 has been amended and claims 2-18 have been added in order to more clearly define the invention.

In the Office Action, the Examiner objected to the disclosure because the text of the first paragraph should be updated with the current status of the cited applications. The Examiner has also rejected Claim 1 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the Applicant regards as the invention. The Examiner also has provisionally rejected claim 1 under 35 U.S.C. § 101 as claiming the same invention as that of claim 1 of copending Application No. 11/679,416. Finally, Examiner has rejected claim 1 on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1 of U.S. Patent No. 7,188,180.

Applicant respectfully traverses the outstanding objection and rejections and requests reconsideration of the subject application in light of the foregoing amendments and the following remarks.

Objection to the Disclosure

In the Office Action, the Examiner objected to the disclosure because the text of the first paragraph should be updated with the current status of the cited applications. The Applicant respectfully submits that Paragraph [0001], as filed, provides the current status of the applications cited therein. Accordingly, the Applicant respectfully requests that the Examiner withdraw this objection.

Rejection of Claim 1 under 35 U.S.C. §112. Second Paragraph

In the Office Action, the Examiner rejected Claim 1 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the Applicant regards as the invention. The Examiner further specified that i) at line 3, it is unclear from where a query message is sent, ii) at line 4, it is unclear from where the query message is requesting a secure computer network address, iii) at line 5, it is unclear where the response message is received and from where the response message is received, and iv) at line 7, it is unclear from where an access request is sent.

Claim 1, as amended, recites:

1. A method of accessing a secure network address, comprising:

 sending a query message from a first network device to a secure domain service, the query message requesting from the secure domain service a secure network address for a second network device;

 receiving at the first network device a response message from the secure domain name service containing the secure network address for the second network device; and

 sending an access request message from the first network device to the secure network address using a virtual private network communication link.

Claim 1 has been amended to include reference to the first and second network devices. The Applicant thus overcomes the Examiner's rejection of Claim 1 under 35 U.S.C. §112, Second Paragraph.

Statutory Type Double Patenting Rejection

The Examiner provisionally rejected claim 1 under 35 U.S.C. § 101 as claiming the same invention as that of claim 1 of copending Application No. 11/679,416. Because claim 1 of copending Application No. 11/679,416 has been cancelled and new claims submitted, the Applicant respectfully submits that this rejection is overcome.

Non-statutory Double Patenting Rejection

The Examiner rejected claim 1 on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1 of U.S. Patent No. 7,188,180.

If the Examiner determines that amended claim 1 of this application should still be rejected on the ground of nonstatutory obvious-type double patenting, applicant will submit a terminal disclaimer.

CONCLUSION

In light of the Amendments and Remarks herein, the Applicant submits that the pending claims, claims 1-19, are in condition for allowance and respectfully requests a notice to this effect. Should the Examiner have any questions, please call the undersigned at the phone number listed below.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 501133 and please credit any excess fees to such deposit account.

Date: December 9, 2009

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

/Toby H. Kusmer/

Toby H. Kusmer
Registration No. 26,418
28 State Street
Boston, MA 02109
Phone: 617-535-4065
Facsimile: 617-535-3800
Date: December 9, 2009
BST99 1638163-2.077580.0066

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

Electronic Patent Application Fee Transmittal

Application Number:	11839987
Filing Date:	16-Aug-2007
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Toby H. Kusmer./Kelly Ciarmataro
Attorney Docket Number:	77580-0066 (VRNK-1 CP2DVCN)

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:				
Extension - 3 months with \$0 paid	1253	1	1110	1110

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				1110

Electronic Acknowledgement Receipt

EFS ID:	6601587
Application Number:	11839987
International Application Number:	
Confirmation Number:	9470
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kelly Ciarmataro
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-0066 (VRNK-1CP2DVCN)
Receipt Date:	09-DEC-2009
Filing Date:	16-AUG-2007
Time Stamp:	13:46:49
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$1110
RAM confirmation Number	36
Deposit Account	501133
Authorized User	

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

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

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	Amendment_A.pdf	96156 250c23c35cbetd509dbb5a0d700329d16b57da54	no	6
Warnings:					
Information:					
2	Fee Worksheet (PTO-875)	fee-info.pdf	30856 05730a38b097e2acfd2a8a5f80439fe7da0460a	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			127012		
<p>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.</p> <p><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.</p> <p><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.</p> <p><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.</p>					



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

Table with columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO., EXAMINER, ART UNIT, PAPER NUMBER, NOTIFICATION DATE, DELIVERY MODE. Includes application details for Victor Larson and examiner LIM, KRISNA.

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):

BostonIPDocket@mwe.com

Art Unit: 2453

1. Claim 1 is still pending for examination, and claims 2-18 are newly added for examination
2. Claim 1 is still rejected on the ground of non-statutory obviousness-type double patenting as being unpatentable over claim 1 of U.S. Patent No. 7, 880,180.

The rejection is respectfully maintained and incorporated by reference as set forth in the last office action.

3. In response to the above rejection, in the remarks, applicants states that the applicants will submit a terminal disclaimer if the Examiner determines that amended claim 1 of this application should still be rejected on the ground of non-statutory obvious-type double patenting.
4. In response to paragraph 3 above, the terminal disclaimer is respectfully requested.
5. Claims 2-18 are objected to as being dependent upon a rejected base claim 1, but would be allowable if the terminal disclaimer is submitted.

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

Art Unit: 2453


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.

kl

December 29, 2009

/Krisna Lim/

Primary Examiner, Art Unit 2453

Index of Claims 	Application/Control No. 11839987	Applicant(s)/Patent Under Reexamination LARSON ET AL.
	Examiner Krisna Lim	Art Unit 2453

✓	Rejected
=	Allowed

-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

Claims renumbered in the same order as presented by applicant
 CPA
 T.D.
 R.1.47

CLAIM		DATE							
Final	Original	06/05/2009	12/29/2009						
	1	✓	✓						
	2		○						
	3		○						
	4		○						
	5		○						
	6		○						
	7		○						
	8		○						
	9		○						
	10		○						
	11		○						
	12		○						
	13		○						
	14		○						
	15		○						
	16		○						
	17		○						
	18		○						

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11839987
	Filing Date	2007-08-16
	First Named Inventor	Larson, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	77580-66(VRNK-1CP2DVCN2)

U.S.PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1	5303302		1994-04-12	Burrows		
	2	5629984		1997-05-13	McManis		

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS							Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1						

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² i	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							<input type="checkbox"/>

If you wish to add additional Foreign Patent Document citation information please click the Add button. Add

NON-PATENT LITERATURE DOCUMENTS								Remove
---------------------------------	--	--	--	--	--	--	--	--------

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11839987	11839987 - GAU: 2453
	Filing Date	2007-08-16	
	First Named Inventor	Larson, et al.	
	Art Unit		
	Examiner Name		
	Attorney Docket Number	77580-66(VRNK-1CP2DVCN2)	

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		<input type="checkbox"/>

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Krisna Lim/	Date Considered	06/05/2009
--------------------	--------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

Subst. for form 1449/PTO SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Complete if Known			
				Application Number		11/839,987	
				Filing Date		August 16, 2007	
				First Named Inventor		Edmund Colby Munger	
				Art Unit		2453	
Examiner Name		Lim, Krisna					
Sheet	1	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)		
U S PATENT DOCUMENTS							
EXAMINER'S INITIALS	CITE NO	Document Number Number-Kind Code ² (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear		
	A1000	5,311,593	05/10/1994	Carmi			
	A1001	5,511,122	04/23/1996	Atkinson			
	A1003	5,805,803	09/08/1998	Birrell et al.			
	A1004	5,822,434	10/13/1998	Caronni et al.			
	A1005	5,898,830	04/27/1999	Wesinger, Jr. et al.			
	A1006	60/134,547	05/17/1999	Victor Sheymov			
	A1007	60/151,563	08/31/1999	Bryan Whittles			
	A1008	5,950,195	09/07/1999	Stockwell et al.			
	A1009	6,119,171	09/12/2000	Alkhatib			
	A1010	6,937,597	08/30/2005	Rosenberg et al.			
	A1011	7,072,964	07/04/2006	Whittle et al.			
	A1012	09/399,753	09/22/1998	Graig Miller et al.			
	A1013	6,079,020	06/20/2000	Liu			
	A1014	6,173,399	01/09/2001	Gilbrech			
	A1015	6,226,748	05/01/2001	Bots et al.			
	A1016	6,226,751	05/01/2001	Arrow et al.			
	A1017	6,701,437	03/02/2004	Hoke et al.			
	A1018	6,055,574	04/25/2000	Smorodinsky et al.			
	A1019	6,246,670	06/12/2001	Karlsson, et al.			
FOREIGN PATENT DOCUMENTS							
EXAMINER'S INITIALS	CITE NO	Foreign Patent Document Country Codes - Number - Kind Codes (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
	B1000	WO 001/17775	03-30-2000	Science Applications International Corporation		Yes	No
	B1001	WO 00/70458	11-23-2000	Comsec Corporation			
	B1002	WO 01/016766	03-08-2001	Science Applications International Corporation			
EXAMINER				DATE CONSIDERED			
/Krisna Lim/				01/03/2010			

*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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known		
				Application Number	11/839,987	
				Filing Date	August 16, 2007	
				First Named Inventor	Edmund Colby Munger	
				Art Unit	2453	
				Examiner Name	Lim, Krisna	
Sheet	2	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)	
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				
	C998	Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009, VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation,				
	C999	Appendix A of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.				
	C1000	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.				
	C1001	1. P. Mockapetris, "DNS Encoding of Network Names and Other Types," Network Working Group, RFC 1101 (April 1989) (RFC1101, DNS SRV)				
	C1002	DNS-related correspondence dated September 7, 1993 to September 20, 1993. (Pre KX, KX Records) [Due to difficulty locating this reference, a copy has not been provided]				
	C1003	R Atkinson, "An Internetwork Authentication Architecture," Naval Research Laboratory, Center for High Assurance Computing Systems (8/5/93). (Atkinson NRL, KX Records)				
	C1004	Henning Schulzrinne, <i>Personal Mobility For Multimedia Services In The Internet</i> , Proceedings of the Interactive Distributed Multimedia Systems and Services European Workshop at 143 (1996). (Schulzrinne 96)				
	C1005	Microsoft Corp., <i>Microsoft Virtual Private Networking: Using Point-to-Point Tunneling Protocol for Low-Cost, Secure, Remote Access Across the Internet</i> (1996) (printed from 1998 PDC DVD-ROM). (Point to Point, Microsoft Prior Art VPN Technology)				
	C1006	"Safe Surfing: How to Build a Secure World Wide Web Connection," IBM Technical Support Organization, (March 1996). (Safe Surfing, WEBSITE ART)				
	C1007	Goldschlag, et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK (May 1996). (Goldschlag II, Onion Routing)				
	C1008	"IPSec Minutes From Montreal", IPSEC Working Group Meeting Notes, http://www.sandleman.ca/ipsec/1996/08/msg00018.html (June 1996) (IPSec Minutes, FreeSWAN)				
	C1009	J M Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California, July 1996. (Galvin, DNSSEC)				
	C1010	J Gilmore, et al. "Re: Key Management, anyone? (DNS Keying)," IPsec Working Group Mailing List Archives (8/96). (Gilmore DNS, FreeSWAN)				
	C1011	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, FreeSWAN)				
	C1012	Arnt Gulbrandsen & Paul Vixie, <i>A DNS RR for specifying the location of services (DNS SRV)</i> , IETF RFC 2052 (October 1996). (RFC 2052, DNS SRV)				
EXAMINER				DATE CONSIDERED		
/Krisna Lim/				01/03/2010		

*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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Complete if Known	
				Application Number	11/839,987
First Named Inventor	Edmund Colby Munger		Art Unit	2453	
Examiner Name	Lim, Krisna		Docket Number	77580-0066 (VRNK-1CP2DVCN)	
Sheet	3	of	17		
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			
	C1013	Freier, et al "The SSL Protocol Version 3.0," Transport Layer Security Working Group (November 18, 1996). (SSL, UNDERLYING SECURITY TECHNOLOGY)			
	C1014	M. Handley, H Schulzrinne, E Schooler, Internet Engineering Task Force, Internet Draft, (12/02/1996) (RFC 2543 Internet Draft 1) [Due to difficulty locating this reference, a copy has not been provided]			
	C1015	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)			
	C1016	Kenneth F Alden & Edward P. Wobber, <i>The AltaVista Tunnel: Using the Internet to Extend Corporate Networks</i> , Digital Technical Journal (1997) (Alden, AltaVista)			
	C1017	Automotive Industry Action Group, "ANX Release 1 Document Publication," AIAG (1997). (AIAG, ANX)			
	C1018	Automotive Industry Action Group, "ANX Release 1 Draft Document Publication," AIAG Publications (1997). (AIAG Release, ANX)			
	C1019	Aventail Corp., "AutoSOCKS v 2.1 Datasheet," available at http://www.archive.org/web/19970212013409/www.aventail.com/prod/autosk2ds.html (1997). (AutoSOCKS, Aventail) [Due to difficulty locating this reference, a copy has not been provided]			
	C1020	Aventail Corp. "Aventail VPN Data Sheet," available at http://www.archive.org/web/19970212013043/www.aventail.com/prod/vpndata.html (1997). (Data Sheet, Aventail)			
	C1021	Aventail Corp., "Directed VPN Vs. Tunnel," available at http://web.archive.org/web/19970620030312/www.aventail.com/educate/directvpn.html (1997). (Directed VPN, Aventail)			
	C1022	Aventail Corp., "Managing Corporate Access to the Internet," Aventail AutoSOCKS White Paper available at http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/ipmwp.html (1997). (Corporate Access, Aventail)			
	C1023	Aventail Corp., "Socks Version 5," Aventail Whitepaper, available at http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/sockswp.html (1997). (Socks, Aventail) [Due to difficulty locating this reference, a copy has not been provided]			
	C1024	Aventail Corp., "VPN Server V2.0 Administration Guide," (1997) (VPN, Aventail)			
	C1025	Goldschlag, et al " <i>Privacy on the Internet</i> ," Naval Research Laboratory, Center for High Assurance Computer Systems (1997). (Goldschlag I, Onion Routing)			
EXAMINER			/Krisna Lim/		DATE CONSIDERED 01/03/2010

*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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Complete if Known	
				Application Number	11/839,987
				Filing Date	August 16, 2007
				First Named Inventor	Edmund Colby Munger
				Art Unit	2453
				Examiner Name	Lim, Krisna
Sheet	4	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)
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.			
	C1026	Microsoft Corp., <i>Installing Configuring and Using PPTP with Microsoft Clients and Servers</i> (1997). (Using PPTP, Microsoft Prior Art VPN Technology)			
	C1027	Microsoft Corp., <i>IP Security for Microsoft Windows NT Server 5.0</i> (1997) (printed from 1998 PDC DVD-ROM). (IP Security, Microsoft Prior Art VPN Technology)			
	C1028	Microsoft Corp., <i>Microsoft Windows NT Active Directory: An Introduction to the Next Generation Directory Services</i> (1997) (printed from 1998 PDC DVD-ROM) (Directory, Microsoft Prior Art VPN Technology)			
	C1029	Microsoft Corp., <i>Routing and Remote Access Service for Windows NT Server New Opportunities Today and Looking Ahead</i> (1997) (printed from 1998 PDC DVD-ROM). (Routing, Microsoft Prior Art VPN Technology)			
	C1030	Microsoft Corp., <i>Understanding Point-to-Point Tunneling Protocol PPTP</i> (1997) (printed from 1998 PDC DVD-ROM). (Understanding PPTP, Microsoft Prior Art VPN Technology)			
	C1031	J Mark Smith et al., <i>Protecting a Private Network: The AltaVista Firewall</i> , Digital Technical Journal (1997). (Smith, AltaVista)			
	C1032	Naganand Doraswamy <i>Implementation of Virtual Private Networks (VPNs) with IP Security</i> , <draft-ietf-ipsec-vpn-00.txt> (March 12, 1997). (Doraswamy)			
	C1033	M Handley, H Schulzrinne, E Schooler, Internet Engineering Task Force, Internet Draft, (03/27/1997). (RFC 2543 Internet Draft 2) [Due to difficulty locating this reference, a copy has not been provided]			
	C1034	Aventail Corp., "Aventail and Cybersafe to Provide Secure Authentication For Internet and Intranet Communication," Press Release, April 3, 1997. (Secure Authentication, Aventail)			
	C1035	D Wagner, et al. "Analysis of the SSL 3.0 Protocol," (April 15, 1997) (Analysis, UNDERLYING SECURITY TECHNOLOGIES)			
	C1036	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)			
	C1037	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)			
	C1038	Aventail Corp., "Aventail Announces the First VPN Solution to Assure Interoperability Across Emerging Security Protocols," June 2, 1997. (First VPN, Aventail)			
EXAMINER			DATE CONSIDERED		
/Krisna Lim/			01/03/2010		

*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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known		
				Application Number	11/839,987	
				Filing Date	August 16, 2007	
				First Named Inventor	Edmund Colby Munger	
				Art Unit	2453	
				Examiner Name	Lim, Krisna	
Sheet	5	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)	
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				
	C1039	Syverson, et al. "Private Web Browsing," Naval Research Laboratory, Center for High 8 Assurance Computer Systems (June 2, 1997). (Syverson, Onion Routing)				
	C1040	Bellcore, "Metrics, Criteria, and Measurement Technique Requirements for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (June 16, 1997). (AIAG Requirements, ANX)				
	C1041	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/31/1997). (RFC 2543 Internet Draft 3) [Due to difficulty locating this reference, a copy has not been provided]				
	C1042	R. Atkinson, "Key Exchange Delegation Record for the DNS," Network Working Group, RFC 2230 (November 1997). (RFC 2230, KX Records)				
	C1043	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/11/1997). (RFC 2543 Internet Draft 4) [Due to difficulty locating this reference, a copy has not been provided]				
	C1044	1998 Microsoft Professional Developers Conference DVD ("1998 PDC DVD-ROM") (including screenshots captured therefrom and produced as MSFTVX 00018827-00018832). (Conference, Microsoft Prior Art VPN Technology)				
	C1045	Microsoft Corp., <i>Virtual Private Networking An Overview</i> (1998) (printed from 1998 PDC DVD-ROM) (Overview, Microsoft Prior Art VPN Technology)				
	C1046	Microsoft Corp., <i>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</i> (1998) (available at http://www.microsoft.com/presspass/features/1998/10-19nt5.mspxptrue). (NT Beta, Microsoft Prior Art VPN Technology)				
	C1047	"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)				
	C1048	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)				
	C1049	R. G. Moskowitz, "Network Address Translation Issues with IPsec," Internet Draft, Internet Engineering Task Force, February 6, 1998. (Moskowitz)				
	C1050	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)				
EXAMINER			/Krisna Lim/	DATE CONSIDERED		
				01/03/2010		

*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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known		
				Application Number	11/839,987	
				Filing Date	August 16, 2007	
				First Named Inventor	Edmund Colby Munger	
				Art Unit	2453	
Examiner Name	Lim, Krisna					
Sheet	6	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)	
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				
	C1051	C. Huitema, 45 al. "Simple Gateway Control Protocol," Version 1 0 (May 5, 1998) (SGCP)				
	C1052	DISA "Secret Internet Protocol Router Network," SIPRNET Program Management Office (D3113) DISN Networks, DISN Transmission Services (May 8, 1998). (DISA, SIPRNET)				
	C1053	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (05/14/1998) (RFC 2543 Internet Draft 5) [Due to difficulty locating this reference, a copy has not been provided]				
	C1054	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (06/17/1998) (RFC 2543 Internet Draft 6) [Due to difficulty locating this reference, a copy has not been provided]				
	C1055	D. McDonald, et al. "PF_KEY Key Management API, Version 2," Network Working Group, RFC 2367 (July 1998). (RFC 2367)				
	C1056	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/16/1998) (RFC 2543 Internet Draft 7) [Due to difficulty locating this reference, a copy has not been provided]				
	C1057	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (08/07/1998). (RFC 2543 Internet Draft 8) [Due to difficulty locating this reference, a copy has not been provided]				
	C1058	Microsoft Corp., <i>Company Focuses on Quality and Customer Feedback</i> (August 18, 1998). (Focus, Microsoft Prior Art VPN Technology)				
	C1059	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (09/18/1998). (RFC 2543 Internet Draft 9) [Due to difficulty locating this reference, a copy has not been provided]				
	C1060	Atkinson, et al. "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998). (RFC 2401, UNDERLYING SECURITY TECHNOLOGIES)				
	C1061	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/12/1998) (RFC 2543 Internet Draft 10) 9 [Due to difficulty locating this reference, a copy has not been provided]				
	C1062	Donald Eastlake, <i>Domain Name System Security Extensions</i> , IETF DNS Security Working Group (December 1998). (DNSSEC-7)				
	C1063	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/15/1998). (RFC 2543 Internet Draft 11) [Due to difficulty locating this reference, a copy has not been provided]				
EXAMINER			DATE CONSIDERED			
/Krisna Lim/			01/03/2010			

*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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	11/839,987
				Filing Date	August 16, 2007
				First Named Inventor	Edmund Colby Munger
				Art Unit	2453
Examiner Name	Lim, Krisna				
Sheet	7	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)
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			
	C1064	Aventail Corp., "Aventail Connect 3 1/2 6 Administrator's Guide," (1999). (Aventail Administrator 3 1, Aventail) [Due to difficulty locating this reference, a copy has not been provided]			
	C1065	Aventail Corp., "Aventail Connect 3 1/2 6 User's Guide," (1999) (Aventail User 3 1, Aventail) [Due to difficulty locating this reference, a copy has not been provided]			
	C1066	Aventail Corp., "Aventail ExtraWeb Server v3 2 Administrator's Guide," (1999) (Aventail ExtraWeb 3 2, Aventail) [Due to difficulty locating this reference, a copy has not been provided]			
	C1067	Kaufman et al, "Implementing IPsec," (Copyright 1999). (Implementing IPSEC, VPN REFERENCES)			
	C1068	Network Solutions, Inc. "Enabling SSL," NSI Registry (1999). (Enabling SSL, UNDERLYING SECURITY TECHNOLOGIES)			
	C1069	Check Point Software Technologies Ltd (1999) (Check Point, Checkpoint FW) [Due to difficulty locating this reference, a copy has not been provided]			
	C1070	Arnt Gulbrandsen & Paul Vixie, <i>A DNS RR for specifying the location of services (DNS SRV)</i> , <draft-ietf-dnsind-rrc2052bis-02.txt> (January 1999). (Gulbrandsen 99, DNS SRV)			
	C1071	C. Scott, et al <i>Virtual Private Networks</i> , O'Reilly and Associates, Inc., 2nd ed (Jan. 1999). (Scott VPNs)			
	C1072	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (01/15/1999) (RFC 2543 Internet Draft 12) [Due to difficulty locating this reference, a copy has not been provided]			
	C1073	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)			
	C1074	H. Schulzrinne, "Internet Telephony: architecture and protocols – an IETF perspective," Computer Networks, Vol. 31, No. 3 (February 1999). (Telephony, Schulzrinne)			
	C1075	M. Handley, et al. "SIP: Session Initiation Protocol," Network Working Group, RFC 2543 and Internet Drafts (12/96-3/99). (Handley, RFC 2543)			
	C1076	FreeSWAN Project, <i>Linux FreeSWAN Compatibility Guide</i> (March 4, 1999). (FreeSWAN Compatibility Guide, FreeSWAN)			
	C1077	Telcordia Technologies, "ANX Release 1 Document Corrections," AIAG (May 11, 1999). (Telcordia, ANX)			
	C1078	Ken Hornstein & Jeffrey Altman, <i>Distributing Kerberos KDC and Realm Information with DNS</i> <draft-ietf-cat-krb-dns-locate-oo.txt> (June 21, 1999). (Hornstein, DNS SRV)			
EXAMINER			DATE CONSIDERED		
/Krisna Lim/			01/03/2010		

*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

(7)
 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./
 Petitioner Apple Inc. - Exhibit 1028, p. 261

Subst. for form 1449/PTO				Complete if Known	
SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Application Number	11/839,987
				Filing Date	August 16, 2007
				First Named Inventor	Edmund Colby Munger
				Art Unit	2453
				Examiner Name	Lim, Krisna
Sheet	8	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)
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			
	C1079	Bhattacharya et. al. "An LDAP Schema for Configuration and Administration of IPsec Based Virtual Private Networks (VPNs)", IETF Internet Draft (October 1999) (Bhattacharya LDAP VPN)			
	C1080	B. Patel, et al. "DHCP Configuration of IPSEC Tunnel Mode," IPSEC Working Group, Internet Draft 02 (10/15/1999). (Patel)			
	C1081	Goncalves, et al. <i>Check Point FireWall -1 Administration Guide</i> , McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW) [Due to difficulty locating this reference, a copy has not been provided]			
	C1082	"Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources," FirstVPN, (Jan 2000). (FirstVPN Microsoft)			
	C1083	Gulbrandsen, Vixie, & Esibov, <i>A DNS RR for specifying the location of services (DNS SRV)</i> , IETF RFC 2782 (February 2000). (RFC 2782, DNS SRV)			
	C1084	MITRE Organization, "Technical Description," Collaborative Operations in Joint Expeditionary Force Experiment (JEFX) 99 (February 2000). (MITRE, SIPRNET)			
	C1085	H Schulzrinne, et al. "Application-Layer Mobility Using SIP," <i>Mobile Computing and Communications Review</i> , Vol. 4, No. 3. pp. 47-57 (July 2000). (Application, SIP)			
	C1086	Kindred et al, "Dynamic VPN Communities: Implementation and Experience," DARPA Information Survivability Conference and Exposition II (June 2001) (DARPA, VPN SYSTEMS)			
	C1087	ANX 101: Basic ANX Service Outline. (Outline, ANX)			
	C1088	ANX 201: Advanced ANX Service. (Advanced, ANX)			
	C1089	Appendix A: Certificate Profile for ANX IPsec Certificates. (Appendix, ANX)			
	C1090	Assured Digital Products. (Assured Digital) [Due to difficulty locating this reference, a copy has not been provided]			
	C1091	Aventail Corp., "Aventail AutoSOCKS the Client Key to Network Security," Aventail Corporation White Paper. (Network Security, Aventail)			
	C1092	Cindy Moran, "DISN Data Networks: Secret Internet Protocol Router Network (SIPRNet)." (Moran, SIPRNET)			
	C1093	Data Fellows F-Secure VPN+ (F-Secure VPN+)			
	C1094	"Interim Operational Systems Doctrine for the Remote Access Security Program (RASP) Secret Dial-In Solution. (RASP, SIPRNET)			
	C1095	<i>Onion Routing</i> , "Investigation of Route Selection Algorithms," available at http://www.onion-router.net/Archives/Route/index.html . (Route Selection, Onion Routing)			
	C1096	Secure Computing, "Bullet-Proofing an Army Net," Washington Technology (Secure, SIPRNET)			
EXAMINER				DATE CONSIDERED	
/Krisna Lim/				01/03/2010	

*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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known		
				Application Number	11/839,987	
				Filing Date	August 16, 2007	
				First Named Inventor	Edmund Colby Munger	
				Art Unit	2453	
				Examiner Name	Lim, Krisna	
Sheet	9	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)	
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				
	C1097	SPARTA "Dynamic Virtual Private Network" (Sparta, VPN SYSTEMS)				
	C1098	Standard Operation Procedure for Using the 1910 Secure Modems. (Standard, SIPRNET)				
	C1099	Publicly available emails relating to FreeS/WAN (MSFTVX00018833-MSFTVX00019206). (FreeS/WAN emails, FreeS/WAN)				
	C1100	Kaufman et al, "Implementing IPsec," (Copyright 1999) (Implementing IPsec)				
	C1101	Network Associates <i>Gauntlet Firewall For Unix User's Guide Version 5.0</i> (1999). (Gauntlet User's Guide - Unix, Firewall Products)				
	C1102	Network Associates <i>Gauntlet Firewall For Windows NT Getting Started Guide Version 5.0</i> (1999) (Gauntlet Getting Started Guide - NT, Firewall Products)				
	C1103	Network Associates <i>Gauntlet Firewall For Unix Getting Started Guide Version 5.0</i> (1999) (Gauntlet Unix Getting Started Guide, Firewall Products)				
	C1104	Network Associates <i>Release Notes Gauntlet Firewall for Unix 5.0</i> (March 19, 1999) (Gauntlet Unix Release Notes, Firewall Products)				
	C1105	Network Associates <i>Gauntlet Firewall For Windows NT Administrator's Guide Version 5.0</i> (1999) (Gauntlet NT Administrator's Guide, Firewall Products)				
	C1106	Trusted Information Systems, Inc <i>Gauntlet Internet Firewall Firewall-to-Firewall Encryption Guide Version 3.1</i> (1996) (Gauntlet Firewall-to-Firewall, Firewall Products)				
	C1107	Network Associates <i>Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0</i> (1999) (Gauntlet NT GVPN, GVPN)				
	C1108	Network Associates <i>Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0</i> (1999) (Gauntlet Unix GVPN, GVPN)				
	C1109	Dan Sterne <i>Dynamic Virtual Private Networks</i> (May 23, 2000) (Sterne DVPN, DVPN)				
	C1110	Darrell Kindred <i>Dynamic Virtual Private Networks (DVPN)</i> (December 21, 1999) (Kindred DVPN, DVPN)				
	C1111	Dan Sterne <i>et al. TIS Dynamic Security Perimeter Research Project Demonstration</i> (March 9, 1998) (Dynamic Security Perimeter, DVPN)				
	C1112	Darrell Kindred <i>Dynamic Virtual Private Networks Capability Description</i> (January 5, 2000) (Kindred DVPN Capability, DVPN) 11				
EXAMINER			DATE CONSIDERED			
/Krisna Lim/			01/03/2010			

*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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	11/839,987
				Filing Date	August 16, 2007
				First Named Inventor	Edmund Colby Munger
				Art Unit	2453
Examiner Name	Lim, Krisna				
Sheet	10	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)
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.			
	C1113	October 7, and 28 1997 email from Domenic J. Turchi Jr (SPARTA00001712-1714, 1808-1811) (Turchi DVPN email, DVPN)			
	C1114	James Just & Dan Sterne <i>Security Quickstart Task Update</i> (February 5, 1997) (Security Quickstart, DVPN)			
	C1115	Virtual Private Network Demonstration dated March 21, 1998 (SPARTA00001844-54) (DVPN Demonstration, DVPN)			
	C1116	GTE Internetworking & BBN Technologies <i>DARPA Information Assurance Program Integrated Feasibility Demonstration (IFD) 1.1 Plan</i> (March 10, 1998) (IFD 1.1, DVPN)			
	C1117	Microsoft Corp Windows NT Server Product Documentation: Administration Guide – Connection Point Services, <i>available at</i> 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.)			
	C1118	Microsoft Corp. Windows NT Server Product Documentation: Administration Kit Guide – Connection Manager, <i>available at</i> 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.)			
	C1119	Microsoft Corp. Autodial Heuristics, <i>available at</i> 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.)			
	C1120	Microsoft Corp., Cariplo: Distributed Component Object Model, (1996) <i>available at</i> http://msdn2.microsoft.com/en-us/library/ms809332(printer).aspx (Cariplo I)			
	C1121	Marc Levy, COM Internet Services (Apr. 23, 1999), <i>available at</i> http://msdn2.microsoft.com/en-us/library/ms809302(printer).aspx (Levy)			
	C1122	Markus Horstmann and Mary Kirtland, DCOM Architecture (July 23, 1997), <i>available at</i> http://msdn2.microsoft.com/en-us/library/ms809311(printer).aspx (Horstmann)			
	C1123	Microsoft Corp., DCOM: A Business Overview (Apr. 1997), <i>available at</i> http://msdn2.microsoft.com/en-us/library/ms809320(printer).aspx (DCOM Business Overview I)			
	C1124	Microsoft Corp., DCOM Technical Overview (Nov. 1996), <i>available at</i> http://msdn2.microsoft.com/en-us/library/ms809340(printer).aspx (DCOM Technical Overview I)			
	C1125	Microsoft Corp., DCOM Architecture White Paper (1998) <i>available in</i> PDC DVD-ROM (DCOM Architecture)			
EXAMINER				DATE CONSIDERED	
/Krisna Lim/				01/03/2010	

*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

(10)
 ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./
 Petitioner Apple Inc. - Exhibit 1028, p. 264

Subst for form 1449/PTO SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known		
				Application Number	11/839,987	
				Filing Date	August 16, 2007	
				First Named Inventor	Edmund Colby Munger	
				Art Unit	2453	
Examiner Name	Lim, Krisna					
Sheet	11	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)	
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				
	C1126	Microsoft Corp, DCOM – The Distributed Component Object Model, A Business Overview White Paper (Microsoft 1997) <i>available in</i> PDC DVD-ROM (DCOM Business Overview II)				
	C1127	Microsoft Corp, DCOM—Cariplo Home Banking Over The Internet White Paper (Microsoft 1996) <i>available in</i> PDC DVD-ROM (Cariplo II)				
	C1128	Microsoft Corp, DCOM Solutions in Action White Paper (Microsoft 1996) <i>available in</i> PDC DVD-ROM (DCOM Solutions in Action)				
	C1129	Microsoft Corp., DCOM Technical Overview White Paper (Microsoft 1996) <i>available in</i> 12 PDC DVD-ROM (DCOM Technical Overview II)				
	C1130	125. Scott Suhy & Glenn Wood, DNS and Microsoft Windows NT 4.0, (1996) <i>available at</i> http://msdn2.microsoft.com/en-us/library/ms810277(printer).aspx (Suhy)				
	C1131	126. Aaron Skonnard, <i>Essential Wininet</i> 313-423 (Addison Wesley Longman 1998) (Essential Wininet)				
	C1132	Microsoft Corp Installing, Configuring, and Using PPTP with Microsoft Clients and Servers, (1998) <i>available at</i> http://msdn2.microsoft.com/enus/library/ms811078(printer).aspx (Using PPTP)				
	C1133	Microsoft Corp., Internet Connection Services for MS RAS, Standard Edition, http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstart.msp (Internet Connection Services I)				
	C1134	Microsoft Corp., Internet Connection Services for RAS, Commercial Edition, <i>available at</i> http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstrtc.msp (Internet Connection Services II)				
	C1135	Microsoft Corp., Internet Explorer 5 Corporate Deployment Guide – Appendix B: Enabling Connections with the Connection Manager Administration Kit, <i>available at</i> http://www.microsoft.com/technet/prodtechnol/ie/deploy/deploy5/appendb.msp (IE5 Corporate Development)				
	C1136	Mark Minasi, <i>Mastering Windows NT Server 4</i> 1359-1442 (6th ed, January 15, 1999)(Mastering Windows NT Server)				
	C1137	<i>Hands On, Self-Paced Training for Supporting Version 4.0</i> 371-473 (Microsoft Press 1998) (Hands On)				
	C1138	Microsoft Corp., MS Point-to-Point Tunneling Protocol (Windows NT 4.0), <i>available at</i> http://www.microsoft.com/technet/archive/winntas/maintain/featusability/pptpwp3.msp (MS PPTP)				
	C1139	Kenneth Gregg, <i>et al</i> , <i>Microsoft Windows NT Server Administrator's Bible</i> 173-206, 883-911, 974-1076 (IDG Books Worldwide 1999) (Gregg)				
	C1140	Microsoft Corp., Remote Access (Windows), <i>available at</i> http://msdn2.microsoft.com/en-us/library/bb545687(VS.85,printer).aspx (Remote Access)				
EXAMINER				DATE CONSIDERED		
				01/03/2010		

*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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known		
				Application Number	11/839,987	
				Filing Date	August 16, 2007	
				First Named Inventor	Edmund Colby Munger	
				Art Unit	2453	
				Examiner Name	Lim, Krisna	
Sheet	12	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)	
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				
	C1141	Microsoft Corp., Understanding PPTP (Windows NT 4.0), available at http://www.microsoft.com/technet/archive/winntas/plan/pptpudst.msp (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.)				
	C1142	Microsoft Corp., Windows NT 4.0: Virtual Private Networking, available at http://www.microsoft.com/technet/archive/winntas/deploy/confeat/vpntwk.msp (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.)				
	C1143	Anthony Northrup, <i>NT Network Plumbing: Routers, Proxies, and Web Services</i> 299-399 (IDG Books Worldwide 1998) (Network Plumbing)				
	C1144	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/rrasch01.msp (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				
	C1145	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.msp (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.)				
	C1146	F-Secure, <i>F-Secure Evaluation Kit</i> (May 1999) (FSECURE 00000003) (Evaluation Kit 3) [Due to difficulty locating this reference, a copy has not been provided]				
	C1147	F-Secure, <i>F-Secure NameSurfer</i> (May 1999) (from FSECURE 00000003) (NameSurfer 3)				
	C1148	F-Secure, <i>F-Secure VPN Administrator's Guide</i> (May 1999) (from FSECURE 00000003) (F-Secure VPN 3)				
	C1149	F-Secure, <i>F-Secure SSH User's & Administrator's Guide</i> (May 1999) (from FSECURE 00000003) (SSH Guide 3)				
	C1150	F-Secure, <i>F-Secure SSH2.0 for Windows NT and 95</i> (May 1999) (from FSECURE 00000003) (SSH 2.0 Guide 3)				
EXAMINER /Krisna Lim/				DATE CONSIDERED 01/03/2010		

*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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>			Complete if Known			
			Application Number		11/839,987	
			Filing Date		August 16, 2007	
			First Named Inventor		Edmund Colby Munger	
			Art Unit		2453	
			Examiner Name		Lim, Krisna	
Sheet	13	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)	
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				
	C1151	F-Secure, <i>F-Secure VPN+ Administrator's Guide</i> (May 1999) (from FSECURE 00000003) (VPN+ Guide 3)				
	C1152	F-Secure, <i>F-Secure VPN+ 4.1</i> (1999) (from FSECURE 00000006) (VPN+ 4.1 Guide 6)				
	C1153	F-Secure, <i>F-Secure SSH</i> (1996) (from FSECURE 00000006) (F-Secure SSH 6)				
	C1154	F-Secure, <i>F-Secure SSH 2.0 for Windows NT and 95</i> (1998) (from FSECURE 00000006) (F-Secure SSH 2.0 Guide 6)				
	C1155	F-Secure, <i>F-Secure Evaluation Kit</i> (Sept. 1998) (FSECURE 00000009) (Evaluation Kit 9) [Due to difficulty locating this reference, a copy has not been provided]				
	C1156	F-Secure, <i>F-Secure SSH User's & Administrator's Guide</i> (Sept 1998) (from FSECURE 00000009) (SSH Guide 9)				
	C1157	F-Secure, <i>F-Secure SSH 2.0 for Windows NT and 95</i> (Sept 1998) (from FSECURE 00000009) (F-Secure SSH 2.0 Guide 9)				
	C1158	F-Secure, <i>F-Secure VPN+</i> (Sept. 1998) (from FSECURE 00000009) (VPN+ Guide 9)				
	C1159	F-Secure, <i>F-Secure Management Tools, Administrator's Guide</i> (1999) (from FSECURE 00000003) (F-Secure Management Tools)				
	C1160	F-Secure, <i>F-Secure Desktop, User's Guide</i> (1997) (from FSECURE 00000009) (FSecure Desktop User's Guide)				
	C1161	SafeNet, Inc , <i>VPN Policy Manager</i> (January 2000) (VPN Policy Manager)				
	C1162	F-Secure, <i>F-Secure VPN+ for Windows NT 4.0</i> (1998) (from FSECURE 00000009) (FSecure VPN+)				
	C1163	IRE, Inc , <i>SafeNet/Soft-PK Version 4</i> (March 28, 2000) (Soft-PK Version 4) [Due to difficulty locating this reference, a copy has not been provided]				
	C1164	IRE/SafeNet Inc , <i>VPN Technologies Overview</i> (March 28, 2000) (Safenet VPN Overview) [Due to difficulty locating this reference, a copy has not been provided]				
	C1165	IRE, Inc , <i>SafeNet / Security Center Technical Reference Addendum</i> (June 22, 1999) (Safenet Addendum)				
EXAMINER			/Krisna Lim/		DATE CONSIDERED 01/03/2010	

*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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known		
				Application Number	11/839,987	
				Filing Date	August 16, 2007	
				First Named Inventor	Edmund Colby Munger	
				Art Unit	2453	
				Examiner Name	Lim, Krisna	
Sheet	14	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)	
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				
	C1166	IRE, Inc., <i>System Description for VPN Policy Manager and SafeNet/SoftPK</i> (March 30, 2000) (VPN Policy Manager System Description)				
	C1167	IRE, Inc., <i>About SafeNet / VPN Policy Manager</i> (1999) (About Safenet VPN Policy Manager)				
	C1168	IRE, Inc., <i>SafeNet/VPN Policy Manager Quick Start Guide Version 1</i> (1999) (SafeNet VPN Policy Manager) [Due to difficulty locating this reference, a copy has not been provided]				
	C1169	Trusted Information Systems, Inc., <i>Gauntlet Internet Firewall, Firewall Product Functional Summary</i> (July 22, 1996) (Gauntlet Functional Summary)				
	C1170	Trusted Information Systems, Inc., <i>Running the Gauntlet Internet Firewall, An Administrator's Guide to Gauntlet Version 3.0</i> (May 31, 1995) (Running the Gauntlet Internet Firewall)				
	C1171	Ted Harwood, <i>Windows NT Terminal Server and Citrix Metaframe</i> (New Riders 1999) (Windows NT Harwood) 79				
	C1172	Todd W. Mathers and Shawn P. Genoway, <i>Windows NT Thin Client Solutions: Implementing Terminal Server and Citrix MetaFrame</i> (Macmillan Technial Publishing 1999) (Windows NT Mathers)				
	C1173	Bernard Aboba et al., <i>Securing L2TP using IPSEC</i> (February 2, 1999)				
	C1174	156 <i>Finding Your Way Through the VPN Maze</i> (1999) ("PGP")				
	C1175	Linux FreeSWAN Overview (1999) (Linux FreeSWAN) Overview)				
	C1176	TimeStep, <i>The Business Case for Secure VPNs</i> (1998) ("TimeStep")				
	C1177	WatchGuard Technologies, Inc., <i>WatchGuard Firebox System Powerpoint</i> (2000) [Due to difficulty locating this reference, a copy has not been provided]				
	C1178	WatchGuard Technologies, Inc., <i>MSS Firewall Specifications</i> (1999) [Due to difficulty locating this reference, a copy has not been provided]				
	C1179	WatchGuard Technologies, Inc., <i>Request for Information, Security Services</i> (2000) [Due to difficulty locating this reference, a copy has not been provided]				
	C1180	WatchGuard Technologies, Inc., <i>Protecting the Internet Distributed Enterprise, White Paper</i> (February 2000) [Due to difficulty locating this reference, a copy has not been provided]				
EXAMINER				DATE CONSIDERED		
/Krisna Lim/				01/03/2010		

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 809 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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known		
				Application Number	11/839,987	
				Filing Date	August 16, 2007	
				First Named Inventor	Edmund Colby Munger	
				Art Unit	2453	
				Examiner Name	Lim, Krisna	
Sheet	15	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)	
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.				
	C1181	WatchGuard Technologies, Inc., <i>WatchGuard LiveSecurity for MSS Powerpoint</i> (Feb. 14 2000)				
	C1182	WatchGuard Technologies, Inc., <i>MSS Version 2.5, Add-On for WatchGuard SOHO Release Notes</i> (July 21, 2000) [Due to difficulty locating this reference, a copy has not been provided]				
	C1183	Air Force Research Laboratory, <i>Statement of Work for Information Assurance System Architecture and Integration, PR No. N-8-6106 (Contract No F30602-98-C-0012)</i> (January 29, 1998)				
	C1184	GTE Internetworking & BBN Technologies <i>DARPA Information Assurance Program Integrated Feasibility Demonstration (IFD) 1.2 Report, Rev. 1.0</i> (September 21, 1998)				
	C1185	BBN Information Assurance Contract, <i>TIS Labs Monthly Status Report</i> (March 16-April 30, 1998)				
	C1186	DARPA, <i>Dynamic Virtual Private Network (VPN) Powerpoint</i>				
	C1187	GTE Internetworking, <i>Contractor's Program Progress Report</i> (March 16-April 30, 1998)				
	C1188	Darrell Kindred, <i>Dynamic Virtual Private Networks (DVPN) Countermeasure Characterization</i> (January 30, 2001)				
	C1189	<i>Virtual Private Networking Countermeasure Characterization</i> (March 30, 2000)				
	C1190	<i>Virtual Private Network Demonstration</i> (March 21, 1998)				
	C1191	Information Assurance/NAI Labs, <i>Dynamic Virtual Private Networks (VPNs) and Integrated Security Management</i> (2000)				
	C1192	Information Assurance/NAI Labs, <i>Create/Add DVPN Enclave</i> (2000)				
	C1193	NAI Labs, <i>IFE 3.1 Integration Demo</i> (2000)				
	C1194	Information Assurance, <i>Science Fair Agenda</i> (2000)				
EXAMINER /Krisna Lim/				DATE CONSIDERED 01/03/2010		

*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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Complete if Known	
				Application Number	11/839,987
				Filing Date	August 16, 2007
				First Named Inventor	Edmund Colby Munger
				Art Unit	2453
				Examiner Name	Lim, Krisna
Sheet	16	of	17	Docket Number	77580-0066 (VRNK-1CP2DVCN)
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			
	C1195	Darrell Kindred et al, <i>Proposed Threads for IFE 3 1</i> (January 13, 2000)			
	C1196	<i>IFE 3 1 Technology Dependencies</i> (2000)			
	C1197	<i>IFE 3 1 Topology</i> (February 9, 2000)			
	C1198	Information Assurance, <i>Information Assurance Integration: IFE 3.1, Hypothesis & Thread Development</i> (January 10-11, 2000)			
	C1199	Information Assurance/NAI Labs, <i>Dynamic Virtual Private Networks Presentation</i> (2000)			
	C1200	Information Assurance/NAI Labs, <i>Dynamic Virtual Private Networks Presentation v. 2</i> (2000)			
	C1201	Information Assurance/NAI Labs, <i>Dynamic Virtual Private Networks Presentation v 3</i> (2000) [Due to difficulty locating this reference, a copy has not been provided]			
	C1202	T. Braun et al, <i>Virtual Private Network Architecture, Charging and Accounting Technology for the Internet</i> (August 1, 1999) (VPNA)			
	C1203	Network Associates Products – <i>PGP Total Network Security Suite, Dynamic Virtual Private Networks</i> (1999)			
	C1204	Microsoft Corporation, <i>Microsoft Proxy Server 2 0</i> (1997) (Proxy Server 2.0, Microsoft Prior Art VPN Technology)			
	C1205	David Johnson et. al, <i>A Guide To Microsoft Proxy Server 2 0</i> (1999) (Johnson, Microsoft Prior Art VPN Technology)			
	C1206	Microsoft Corporation, <i>Setting Server Parameters</i> (1997 (copied from Proxy Server 2 0 CD labeled MSFTVX00157288) (Setting Server Parameters, Microsoft Prior Art VPN Technology)			
	C1207	Kevin Schuler, <i>Microsoft Proxy Server 2</i> (1998) (Schuler, Microsoft Prior Art VPN Technology)			
	C1208	Erik Rozell et al, <i>MCSE Proxy Server 2 Study Guide</i> (1998) (Rozell, Microsoft Prior 15 Art VPN Technology)			
EXAMINER			DATE CONSIDERED		
/Krisna Lim/			01/03/2010		

*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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Complete if Known	
				Application Number	11/839,987
				Filing Date	August 16, 2007
				First Named Inventor	Edmund Colby Munger
				Art Unit	2453
				Examiner Name	Lim, Krisna
Sheet	17	of	17	Docket Number	77580-0066 (VRNK-1CP2DVVN)
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.			
	C1209	M. Shane Stigler & Mark A Linsenhardt, <i>IIS 4 and Proxy Server 2</i> (1999) (Stigler, Microsoft Prior Art VPN Technology)			
	C1210	David G. Schaer, <i>MCSE Test Success: Proxy Server 2</i> (1998) (Schaer, Microsoft Prior Art VPN Technology)			
	C1211	John Savill, <i>The Windows NT and Windows 2000 Answer Book</i> (1999) (Savill, Microsoft Prior Art VPN Technology)			
	C1212	Network Associates <i>Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0</i> (1999) (Gauntlet NT GVPN, GVPN)			
	C1213	Network Associates <i>Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0</i> (1999) (Gauntlet Unix GVPN, GVPN)			
	C1214	File History for U.S. Application Serial No. 09/653,201, Applicant(s): Whittle Bryan, et al., Filing Date 08/31/2000.			
	C1215	<i>AutoSOCKS v2.1</i> , Datasheet, http://web.archive.org/web/19970212013409/www.aventail.com/prod/autoskds.html			
	C1216	Ran Atkinson, <i>Use of DNS to Distribute Keys</i> , 7 Sept 1993, http://ops.ietf.org/lists/namedroppers/namedroppers.199x/msg00945.html			
	C1217	FirstVPN Enterprise Networks, Overview			
	C1218	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			
	C1219	The TLS Protocol Version 1.0; January 1999; page 65 of 71			
	C1220	Elizabeth D. Zwicky, et al., <i>Building Internet Firewalls</i> , 2nd Ed.			
	C1221	Virtual Private Networks – Assured Digital Incorporated – ADI 4500; http://web.archive.org/web/19990224050035/www.assured-digital.com/products/prodvpn/adia4500.htm			
	C1222	Accessware – The Third Wave in Network Security, Conclave from Internet Dynamics; http://web.archive.org/web/11980210013830/interdyn.com/Accessware.html			
	C1223	Extended System Press Release, Sept 2, 1997; <i>Extended VPN Uses The Internet to Create Virtual Private Networks</i> , www.extendedsystems.com			
	C1224	Socks Version 5; Executive Summary; http://web.archive.org/web/199970620031945/www.aventail.com/educate/whitepaper/socks/wp.html			
	C1225	Internet Dynamics First to Ship Integrated Security Solutions for Enterprise Intranets and Extranets; Sept. 15, 1997; http://web.archive.org/web/19980210014150/interdyn.com			
	C1226	Emails from various individuals to Linux IPsec re: DNS-LDAP Splicing			
EXAMINER				DATE CONSIDERED	
/Krisna Lim/				01/03/2010	

*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

BS199 1623736-1 077580 0066

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Subst. for form 1449/PTO		Complete if Known	
				Application Number		11/839,987	
				Filing Date		August 16, 2007	
				First Named Inventor		Victor Larson	
				Art Unit		2453	
Examiner Name		Lim, Krisna					
Sheet	1	of	2	Docket Number	77580-0066 (VRNK-1CP2DVCN2)		
U.S. PATENT DOCUMENTS							
EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code: <i>(if known)</i>	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear		
FOREIGN PATENT DOCUMENTS							
EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes -Number 4 -Kind Codes <i>(if known)</i>	Publication Date MM-DD-YYYY	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.					
	C1002	DNS-related correspondence dated September 7, 1993 to September 20, 1993. (Pre KX, KX Records)					
	C1014	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/02/1996). (RFC 2543 Internet Draft 1)					
	C1019	Aventail Corp., "AutoSOCKS v. 2.1 Datasheet," available at http://www.archive.org/web/19970212013409/www.aventail.com/prod/autosk2ds.html (1997). (AutoSOCKS, Aventail)					
	C1023	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)					
	C1033	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (03/27/1997). (RFC 2543 Internet Draft 2)					
	C1041	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/31/1997). (RFC 2543 Internet Draft 3)					
	C1043	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/11/1997). (RFC 2543 Internet Draft 4)					
	C1053	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (05/14/1998). (RFC 2543 Internet Draft 5)					
	C1054	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (06/17/1998). (RFC 2543 Internet Draft 6)					
	C1056	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/16/1998). (RFC 2543 Internet Draft 7)					
	C1057	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (08/07/1998). (RFC 2543 Internet Draft 8)					
	C1059	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (09/18/1998). (RFC 2543 Internet Draft 9)					
EXAMINER /Krisna Lim/				DATE CONSIDERED 01/03/2010			

*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.

(1)
ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./
Petitioner Apple Inc. - Exhibit 1028, p. 273

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Subst. for form 1449/PTO		Complete if Known		
				Application Number	11/839,987		Filing Date	August 16, 2007
Sheet				2 of 2		First Named Inventor	Victor Larson	
						Art Unit	2453	
Sheet				2 of 2		Examiner Name	Lim, Krisna	
						Docket Number	77580-0066 (VRNK-1CP2DVCN2)	
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.						
	C1061	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/12/1998). (RFC 2543 Internet Draft 10)						
	C1063	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/15/1998). (RFC 2543 Internet Draft 11)						
	C1064	Aventail Corp., "Aventail Connect 3.1/2.6 Administrator's Guide," (1999). (Aventail Administrator 3.1, Aventail)						
	C1065	Aventail Corp., "Aventail Connect 3.1/2.6 User's Guide," (1999). (Aventail User 3.1, Aventail)						
	C1066	Aventail Corp., "Aventail ExtraWeb Server v3.2 Administrator's Guide," (1999). (Aventail ExtraWeb 3.2, Aventail)						
	C1069	Check Point Software Technologies Ltd. (1999) (Check Point, Checkpoint FW)						
	C1072	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (01/15/1999). (RFC 2543 Internet Draft 12)						
	C1081	Goncalves, et al. <i>Check Point FireWall -1 Administration Guide</i> , McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW)						
	C1090	Assured Digital Products. (Assured Digital)						
	C1146	F-Secure, <i>F-Secure Evaluation Kit</i> (May 1999) (FSECURE 00000003) (Evaluation Kit 3)						
	C1155	F-Secure, <i>F-Secure Evaluation Kit</i> (Sept. 1998) (FSECURE 00000009) (Evaluation Kit 9)						
	C1163	IRE, Inc., <i>SafeNet/Soft-PK Version 4</i> (March 28, 2000) (Soft-PK Version 4)						
	C1164	IRE/SafeNet Inc., <i>VPN Technologies Overview</i> (March 28, 2000) (Safenet VPN Overview)						
	C1168	IRE, Inc., <i>SafeNet/VPN Policy Manager Quick Start Guide Version 1</i> (1999) (SafeNet VPN Policy Manager)						
	C1201	Information Assurance/NAI Labs, <i>Dynamic Virtual Private Networks Presentation v.3</i> (2000)						
EXAMINER				/Krisna Lim/		DATE CONSIDERED		01/03/2010

*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.

BST99 1629426-1.077580.0066

(2)

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./
Petitioner Apple Inc. - Exhibit 1028, p. 274

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11839987
	Filing Date	2007-08-16
	First Named Inventor	Larson, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	77580-66(VRNK-1CP2DVCN2)

U.S.PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1	5771239		1998-06-23	Moroney, et al.		

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

U.S.PATENT APPLICATION PUBLICATIONS							Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1						

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							<input type="checkbox"/>

If you wish to add additional Foreign Patent Document citation information please click the Add button

Add

NON-PATENT LITERATURE DOCUMENTS				Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		11839987	11839987 - GAU: 2453
	Filing Date		2007-08-16	
	First Named Inventor	Larson, et al.		
	Art Unit			
	Examiner Name			
	Attorney Docket Number		77580-66(VRNK-1CP2DVCN2)	

1	FASBENDER, A., et al., Variable and Scalable Security: Protection of Location Information in Mobile IP, IEEE VTS, 46th, 1996, 5 pp.	<input type="checkbox"/>
---	---	--------------------------

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Krisna Lim/	Date Considered	06/05/2009
--------------------	--------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		11839987	
	Filing Date		2007-08-16	
	First Named Inventor	Larson, et al.		
	Art Unit			
	Examiner Name			
	Attorney Docket Number		77580-66(VRNK-1CP2DVCN2)	

U.S.PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1	5384848		1995-01-00	Kikuchi		
	2	6223287		2001-04-00	Douglas, et al.		

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS							Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1						

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² j	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							<input type="checkbox"/>

If you wish to add additional Foreign Patent Document citation information please click the Add button. Add

NON-PATENT LITERATURE DOCUMENTS							Remove
---------------------------------	--	--	--	--	--	--	--------

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11839987	11839987 - GAU: 2453
	Filing Date	2007-08-16	
	First Named Inventor	Larson, et al.	
	Art Unit		
	Examiner Name		
	Attorney Docket Number	77580-66(VRNK-1CP2DVCN2)	

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		<input type="checkbox"/>


If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Krisna Lim/	Date Considered	06/05/2009
--------------------	--------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

Search Notes 	Application/Control No. 11839987	Applicant(s)/Patent Under Reexamination LARSON ET AL.
	Examiner Krisna Lim	Art Unit 2453

SEARCHED			
Class	Subclass	Date	Examiner
709	225-229, 245	12/29/09	kl

SEARCH NOTES		
Search Notes	Date	Examiner
EAST, Inventors	6/5/09	kl

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

--	--

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.

Request For Continued Examination (RCE) Transmittal

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

Application Number	11/839,987
Filing Date	August 16, 2007
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Lim, Krisna
Attorney Docket Number	77580-066 (VRNK-1CP2DVCN2)


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. See Instruction Sheet for RCEs (not to be submitted to the USPTO) on page 2.

1. 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).
- a. 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.
- i. Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ii. Other _____
- b. Enclosed
- i. Amendment/Reply iii. Information Disclosure Statement (IDS)
- ii. Affidavit(s)/Declaration(s) iv. Other Form 1449 (3 pages)
2. Miscellaneous _____
- a. 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)
- b. Other _____
3. Fees The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.
- a. The Director is hereby authorized to charge the following fees, any underpayment of fees, or credit any overpayments to Deposit Account No. 50-1133
- i. RCE fee required under 37 CFR 1.17(e)
- ii. Extension of time fee (37 CFR 1.136 and 1.17)
- iii. Other Terminal Disclaimer Fee \$140.00
- b. Check in the amount of \$ _____ enclosed
- c. Payment by credit card (Form PTO-2038 enclosed)

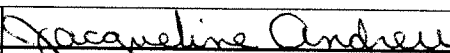
WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Signature		Date	January 8, 2010
Name (Print / Type)	Atabak R. Royace	Registration No.	59,037

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop RCE, Commissioner For Patents, P.O. Box 1450, Alexandria, VA 22313-1450 or facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.

Signature		Date	January 8, 2010
Name (Print / Type)	Jacqueline Andreu	Date	January 8, 2010

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing the burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

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

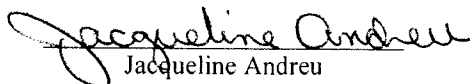
PATENT

Attorney Docket No. 077580-0066 (VRNK-1CP2DVCN2)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Victor Larson et al.
Application Serial No.: 11/839,987
Filing Date: August 16, 2007
Title: METHOD FOR ESTABLISHING SECURE COMMUNICATION
LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE
NETWORK
Examiner: Lim, Krisna
Art Unit: 2453
Confirmation No.: 9470
Atty. Docket No.: 077580-0066 (VRNK-1CP2DVCN2)

I hereby certify that this correspondence is being electronically transmitted to the United States Patent and Trademark Office via ESF-WEB on January 8, 2010.


Jacqueline Andreu

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

RESPONSE TO FINAL OFFICE ACTION

In response to the final Office Action mailed January 6, 2010 (“the Office Action”), please consider the following remarks.

Remarks begin on page 2 of this paper.

Remarks

Applicant appreciates the Examiner's examination of the subject application. Claims 1-18 are currently pending. The only prosecution issue that is remaining in this application is the following rejection.

Non-statutory Double Patenting Rejection

The Examiner rejects claim 1 on the ground of non-statutory obviousness-type double patenting and objects to claims 2-18 as being dependent upon rejected claim 1. The Examiner states that claim 1 is "still rejected . . . as being unpatentable over claim 1 of U.S. Patent No. 7,880,180."

Applicant respectfully submits that the above-referenced patent number is incorrect. The correct patent number should be U.S. Patent No. 7,188,180. The 7,188,180 patent was also cited by the Examiner in the Office Action dated 06/09/2009 in connection with the same rejection.

To overcome the rejection and the related objections, Applicant herewith submits a Terminal Disclaimers for U.S. Patent No. 7,188,180, linking the instant application to that patent. Accordingly, withdrawal of this rejection is respectfully requested.

CONCLUSION

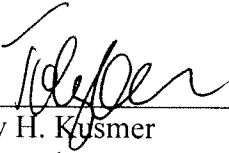
In light of the Remarks herein, the Applicant submits that the pending claims, claims 1-18, are in condition for allowance and respectfully requests a notice to this effect. Should the Examiner have any questions, please call the undersigned at the phone number listed below.

Serial No.: 11/839,987
Response to Jan. 06, 2010 Office Action

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.

The Commissioner for Patents is authorized to charge any fees required under 37 C.F.R. 1.20(d), for the terminal disclaimer filed herewith, to deposit account 50-1133

Respectfully submitted,
McDERMOTT WILL & EMERY LLP



Toby H. Kusmer
Registration No. 26,418
28 State Street
Boston, MA 02109
Phone: 617-535-4065
Facsimile: 617-535-3800

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

Date: January 8, 2010
BST99 1640177-1.077580.0066

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 OBTAIN A DOUBLE PATENTING
REJECTION OVER A "PRIOR" PATENT**

Docket Number (Optional)

077580-0066 (VRNK-1CP2DVCN2)

In re Application of: Larson et al.

Application No.: 11/839,987

Filed: August 16, 2007

For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

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 prior patent No. 7,188,180 as the term of said prior patent is defined in 35 U.S.C. 154 and 173, and 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 as defined in 35 U.S.C. 154 and 173 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



Signature

January 8, 2010

Date

Toby Kusmer

Typed or printed name

617-535-4065

Telephone Number

- Terminal disclaimer fee under 37 CFR 1.20(d) included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Munger et al.

Customer No.: 23,630

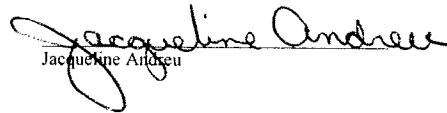
Appl. No. : 11/839,987

Confirmation No.: 9470

Filed : August 16, 2007

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this correspondence is being electronically-transmitted to the United States Patent and Trademark Office on January 8, 2010.


Jacqueline Andree

Title : METHOD FOR ESTABLISHING
SECURE COMMUNICATION LINK
BETWEEN COMPUTERS OF
VIRTUAL PRIVATE NETWORK

Grp./A.U. : 2453

Examiner: : LIM, Krisna

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

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT
UNDER 37 C.F.R. § 1.97(b)

Sir:

In accordance with the provisions of 37 C.F.R. 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the documents listed on the attached form PTO-1449. It is respectfully requested that the documents be expressly considered during the prosecution of this application, and that the documents be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement is being filed concurrently with filing of an RCE. Accordingly, no fee is believed to be due for filing of this IDS. The Commissioner is authorized to charge the required RCE fee and any other fees due in connection with the filing of this IDS to our Deposit Account No. 50-1133.

References Nos. C1227-C1239 listed in the attached form PTO-1449 were submitted on November 6, 2009, and references Nos. C1240-C1243 were submitted on December 14, 2009, to the U.S. Patent and Trademark Office in parent application No. 11/679,416, filed Feb. 27, 2007, which is relied upon for an earlier filing date under 35 USC 120 (the above-identified application is a continuation of application No. 11/679,416). In accordance with 37 C.F.R. § 1.98(d), copies of these references are not attached. Applicants will be pleased to provide copies of the references if requested by the Examiner.

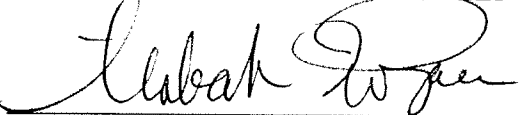
The Examiner is invited to contact the undersign agent for any questions and/or copies of references.

This Statement is not to be interpreted as a representation that the cited publications are material, that an exhaustive search has been conducted, or that no other relevant information exists. Nor shall the citation of any publication herein be construed *per se* as a representation that such publication is prior art. Moreover, the Applicants understand that the Examiner will make an independent evaluation of the cited publications.

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



Atabak R. Royae
Registration No. 59,037
28 State Street
Boston, MA 02109
Phone: 617-535-4108
Facsimile: 617-535-3800
Date: January 8, 2010

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

BST99 1640172-1.077580.0066

Subst. for form 1449/PTO				Complete if Known		
SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Application Number	11/839,987	
				Filing Date	August 16, 2007	
				First Named Inventor	Victor Larson	
				Art Unit	2453	
				Examiner Name	LIM, Krisna	
Sheet	1	of	2	Docket Number	077580-0066 (VRNK-1CP2DVCN2)	
U.S. PATENT DOCUMENTS						
EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code ² (if known)	Publication Date MM-DD-YYYY	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 Code ³ -Number 4-Kind Codes (if known)	Publication Date MM-DD-YYYY	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.				
	C1227	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				
	C1228	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				
	C1229	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				
	C1230	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				
	C1231	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				
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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known		
				Application Number	11/839,987	
				Filing Date	August 16, 2007	
				First Named Inventor	Victor Larson	
				Art Unit	2453	
Examiner Name	LIM, Krisna					
Sheet	2	of	2	Docket Number	077580-0066 (VRNK-1CP2DVCN2)	
OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)						
	C1232	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				
	C1233	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				
	C1234	Derrell Piper, "The Internet IP Security Domain of Interpretation for ISAKMP," RFC 2407 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html				
	C1235	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				
	C1236	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				
	C1237	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				
	C1238	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				
	C1239	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")				
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.

BST99 1640187-1.077580.0066

Subst. for form 1449/PTO SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known		
				Application Number	11/839,987	
				Filing Date	August 16, 2007	
				First Named Inventor	Victor Larson	
				Art Unit	2453	
Examiner Name	LIM, Krisna					
Sheet	1	of	1	Docket Number	077580-0066 (VRNK-1CP2DVCN2)	

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code ² (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1019	US 7,461,334	12/02/08	Lu, et al.	
	A1020	US 7,353,841	04/08/08	Kono, et al.	
	A1021	US 7,188,175	03/06/07	McKeeth, James A.	
	A1022	US 7,167,904	01/23/07	Devarajan, et al.	
	A1023	US 7,039,713	05/02/06	Van Gunter, et al.	
	A1024	US 6,757,740	06/29/04	Parekh, et al.	
	A1025	US 6,752,166	06/22/04	Lull, et al.	
	A1026	US 6,687,746	02/03/04	Shuster, et al.	
	A1027	US 6,338,082	01/08/02	Schneider, Eric	
	A1028	US 6,333,272	12/25/01	McMillin, et al.	
	A1029	US 6,314,463	11/06/01	Abbott, et al.	
	A1030	US 6,298,341	10/02/01	Mann, et al.	
	A1031	US 6,262,987	07/17/01	Mogul, Jeffrey C.	
	A1032	US 6,199,112	03/06/04	Wilson, Stephen K.	
	A1033	US 2,895,502	07/21/59	Garland Roper Charles, et al.	
	A1034	US 2001/0049741	12/06/01	Skene, et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code ³ -Number 4-Kind Codes (if known)	Publication Date MM-DD-YYYY	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.
	C1240	David Kosiur, "Building and Managing Virtual Private Networks" (1998)
	C1241	P. Mockapetris, "Domain Names - Implementation and Specification," Network Working Group, RFC 1035 (November 1987)
	C1242	Request for Inter Partes Reexamination of Patent No. 6,502,135, dated Nov. 25, 2009.
	C1243	Request for Inter Partes Reexamination of Patent No. 7,188,180, dated Nov. 25, 2009.

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.

BST99 1640184-1.077580.0066

Electronic Patent Application Fee Transmittal

Application Number:	11839987
Filing Date:	16-Aug-2007
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Atabak R Royae/Jacqueline Andreu
Attorney Docket Number:	77580-0066 (VRNK-1 CP2DVCN)

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	810	810
Statutory disclaimer	1814	1	140	140
Total in USD (\$)				950

Electronic Acknowledgement Receipt

EFS ID:	6777934
Application Number:	11839987
International Application Number:	
Confirmation Number:	9470
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Atabak R Royae/Jacqueline Andreu
Filer Authorized By:	Atabak R Royae
Attorney Docket Number:	77580-0066 (VRNK-1CP2DVCN)
Receipt Date:	08-JAN-2010
Filing Date:	16-AUG-2007
Time Stamp:	16:28:18
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$950
RAM confirmation Number	2916
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 1.21 (Miscellaneous fees and charges)

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	RCE.pdf	94540 cb1fa95957fd852f4f0c54cc28cc54b2ecef4092	no	1
Warnings:					
This is not a USPTO supplied RCE SB30 form.					
Information:					
2	Amendment After Final	Response.pdf	85299 fd76b370e36de9170926689cb535565bc3e7a7b8e	no	3
Warnings:					
Information:					
3	Terminal Disclaimer Filed	Disclaimer.pdf	75140 27cc0401d468f83819d1c824fe2f6fbc379ca223	no	1
Warnings:					
Information:					
4	Transmittal Letter	IDSSstatement.pdf	79889 46e7b9033dd961d63dbac2c3729f815cca7475eb	no	2
Warnings:					
Information:					
5	Information Disclosure Statement (IDS) Filed (SB/08)	IDS.pdf	234456 da46604fea5dcf95fa91adee548d40111c6c1fa2	no	3
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
6	Fee Worksheet (PTO-875)	fee-info.pdf	32356 cb896d4cbd74796cdd043f60ee43a170ccb6bebfa	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			601680		

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.

Entered ^W/RCE

dtd 1/8/10

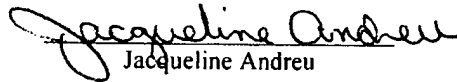
PATENT
Attorney Docket No. 077580-0066 (VRNK-1CP2DVCN2)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Victor Larson et al.
Application Serial No.: 11/839,987
Filing Date: August 16, 2007
Title: METHOD FOR ESTABLISHING SECURE COMMUNICATION
LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE
NETWORK
Examiner: Lim, Krisna
Art Unit: 2453
Confirmation No.: 9470
Atty. Docket No.: 077580-0066 (VRNK-1CP2DVCN2)

AMK
1/13/10

I hereby certify that this correspondence is being electronically transmitted to the United States Patent and Trademark Office via ESF-WEB on January 8, 2010.



Jacqueline Andreu

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

RESPONSE TO FINAL OFFICE ACTION

In response to the final Office Action mailed January 6, 2010 ("the Office Action"), please consider the following remarks.

Remarks begin on page 2 of this paper.

Application Number 	Application/Control No. 11/839,987	Applicant(s)/Patent under Reexamination LARSON ET AL.

Document Code - DISQ	Internal Document – DO NOT MAIL
-----------------------------	--

TERMINAL DISCLAIMER	<input checked="" type="checkbox"/> APPROVED	<input type="checkbox"/> DISAPPROVED
Date Filed : 1/8/10	This patent is subject to a Terminal Disclaimer	

Approved/Disapproved by:
Felicia D. Roberts 7,188,180

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 02/24/2010

MCDERMOTT WILL & EMERY LLP
28 STATE STREET
BOSTON, MA 02109-1775

EXAMINER
LIM, KRISNA
ART UNIT PAPER NUMBER

2453
DATE MAILED: 02/24/2010

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.

11/839,987 08/16/2007 Victor Larson 77580-0066 9470

TITLE OF INVENTION: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

Table with 7 columns: APPLN. TYPE, SMALL ENTITY, ISSUE FEE DUE, PUBLICATION FEE DUE, PREV. PAID ISSUE FEE, TOTAL FEE(S) DUE, DATE DUE

nonprovisional NO \$1510 \$300 \$0 \$1810 05/24/2010

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 SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

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 02/24/2010

MCDERMOTT WILL & EMERY LLP
 28 STATE STREET
 BOSTON, MA 02109-1775

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.
-----------------	-------------	----------------------	---------------------	------------------

11/839,987 08/16/2007 Victor Larson 77580-0066 9470

TITLE OF INVENTION: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
-------------	--------------	---------------	---------------------	----------------------	------------------	----------

nonprovisional NO \$1510 \$300 \$0 \$1810 05/24/2010

EXAMINER	ART UNIT	CLASS-SUBCLASS
----------	----------	----------------

LIM, KRISNA 2453 709-227000

<p>1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).</p> <p><input type="checkbox"/> Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.</p> <p><input type="checkbox"/> "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.</p>	<p>2. For printing on the patent front page, list</p> <p>(1) the names of up to 3 registered patent attorneys or agents OR, alternatively, 1 _____</p> <p>(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. 2 _____</p> <p>3 _____</p>
---	---

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

<p>4a. The following fee(s) are submitted:</p> <p><input type="checkbox"/> Issue Fee</p> <p><input type="checkbox"/> Publication Fee (No small entity discount permitted)</p> <p><input type="checkbox"/> Advance Order - # of Copies _____</p>	<p>4b. Payment of Fee(s); (Please first reapply any previously paid issue fee shown above)</p> <p><input type="checkbox"/> A check is enclosed.</p> <p><input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.</p> <p><input type="checkbox"/> The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).</p>
---	--

5. Change in Entity Status (from status indicated above)

a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information 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.



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

Table with columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
11/839,987 08/16/2007 Victor Larson 77580-0066 9470
23630 7590 02/24/2010
MCDERMOTT WILL & EMERY LLP
28 STATE STREET
BOSTON, MA 02109-1775
EXAMINER LIM, KRISNA
ART UNIT 2453 PAPER NUMBER
DATE MAILED: 02/24/2010

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 145 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 145 day(s).

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 Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Notice of Allowability

Application No.	Applicant(s)	
11/839,987	LARSON ET AL.	
Examiner	Art Unit	
Krisna Lim	2453	

-- 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 1/8/2010.
- 2. The allowed claim(s) is/are 1-18.
- 3. Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some* c) None of 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.

- 4. A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 - 5. CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) hereto or 2) to Paper No./Mail Date _____.
 - (b) 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. Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3. Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
- 4. Examiner's Comment Regarding Requirement for Deposit of Biological Material
- 5. Notice of Informal Patent Application
- 6. Interview Summary (PTO-413), Paper No./Mail Date _____.
- 7. Examiner's Amendment/Comment
- 8. Examiner's Statement of Reasons for Allowance
- 9. Other _____.

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:

The prior arts of record do not teach or suggest a system and a method for accessing a secure computer network address comprising steps of: sending a query message requesting for a secure computer network address from a secure domain name service; and using a virtual private network communication link to send an access request message to the secure computer network address.

The examiner considers the applicants' claims 1-18 to be allowable based on the claim interpretation and the aforesaid prior arts of record.

Any comments considered necessary by applicant must be submitted no later than the payment of the Issue Fee and, to avoid processing delays, should preferably **accompany** the Issue Fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

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, Joseph Thomas, can be reached on 571-272-6776. 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

Application/Control Number: 11/839,987

Page 3

Art Unit: 2453

Business Center (EBC) at 866-217-9197 (toll-free).

KI

February 13, 2010

/Krisna Lim/

Primary Examiner, Art Unit 2453

Notice of References Cited	Application/Control No. 11/839,987	Applicant(s)/Patent Under Reexamination LARSON ET AL.	
	Examiner Krisna Lim	Art Unit 2453	Page 1 of 1

U.S. PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A US-6,061,346	05-2000	Nordman, Mikael	370/352
*	B US-6,557,037	04-2003	Provino, Joseph E.	709/227
*	C US-6,202,081	03-2001	Naudus, Stanley T.	709/200
	D US-			
	E US-			
	F US-			
	G US-			
	H US-			
	I US-			
	J US-			
	K US-			
	L US-			
	M US-			


FOREIGN PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N				
	O				
	P				
	Q				
	R				
	S				
	T				

NON-PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)				
	U				
	V				
	W				
	X				

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims 	Application/Control No. 11839987	Applicant(s)/Patent Under Reexamination LARSON ET AL.
	Examiner Krisna Lim	Art Unit 2453

✓	Rejected
=	Allowed

-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

Claims renumbered in the same order as presented by applicant
 CPA
 T.D.
 R.1.47

CLAIM		DATE							
Final	Original	06/05/2009	12/29/2009	02/13/2010					
	1	✓	✓	=					
	2		○	=					
	3		○	=					
	4		○	=					
	5		○	=					
	6		○	=					
	7		○	=					
	8		○	=					
	9		○	=					
	10		○	=					
	11		○	=					
	12		○	=					
	13		○	=					
	14		○	=					
	15		○	=					
	16		○	=					
	17		○	=					
	18		○	=					

Subst. for form 1449/PTO SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Complete if Known			
				Application Number	11/839,987		
				Filing Date	August 16, 2007		
				First Named Inventor	Victor Larson		
				Art Unit	2453		
				Examiner Name	LIM, Krisna		
Sheet	1	of	2	Docket Number	077580-0066 (VRNK-1CP2DVCN2)		
U.S. PATENT DOCUMENTS							
EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code ² (if known)	Publication Date MM-DD-YYYY	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 Code ³ -Number ⁴ -Kind Codes (if known)	Publication Date MM-DD-YYYY	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.					
	C1227	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					
	C1228	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					
	C1229	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					
	C1230	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					
	C1231	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					
EXAMINER /Krisna Lim/				DATE CONSIDERED 02/13/2010			

*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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known			
				Application Number		11/839,987	
				Filing Date		August 16, 2007	
				First Named Inventor		Victor Larson	
				Art Unit		2453	
				Examiner Name		LIM, Krisna	
Sheet	2	of	2	Docket Number	077580-0066 (VRNK-1CP2DVCN2)		
OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)							
	C1232	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					
	C1233	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					
	C1234	Derrell Piper, "The Internet IP Security Domain of Interpretation for ISAKMP," RFC 2407 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html					
	C1235	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					
	C1236	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					
	C1237	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					
	C1238	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					
	C1239	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")					
EXAMINER			DATE CONSIDERED				
/Krisna Lim/			02/13/2010				

*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.

BST99 1640187-1.077580.0066

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	8801	secure same network same address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/02/13 12:21
L2	3277	secure same domain same (name or service)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/02/13 12:22
L3	896	l1 and l2	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/02/13 12:22
L4	81	l3 and ((secure same domain same name) or SDN).ti,ab,clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/02/13 12:23
L5	38499	((virtual same private same network) or VPN)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/02/13 12:23
L6	441	l5 and l3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/02/13 12:24
L7	0	l6 and (access\$4 same secure same network same address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/02/13 12:24

L8	0	l6 and (access same secure same network same address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/02/13 12:25
L9	0	(access\$4 same secure same network same address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/02/13 12:25
L10	4131	(access\$4 same secure same network same address)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/02/13 12:26
L11	276	l10 and l6	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/02/13 12:26
L12	6	l11 and @ad<="19981030"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/02/13 12:27
L13	18787	709/225-229.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/02/13 12:29
L14	391	l10 and l13	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/02/13 12:30
L15	27	l14 and @ad<="19981030"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/02/13 12:30

L16	64826	establish\$4 same secur\$4 same (link or communication or network)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/02/13 12:39
L17	487	l16 and l3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/02/13 12:39
L18	10	l17 and @ad<="19981030"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/02/13 12:39
L19	49	((VICTOR) near2 (LARSON)). INV.	US-PGPUB; USPAT; USOCR	OR	ON	2010/02/13 12:42
L20	169	((ROBERT) near2 (SHORT)). INV.	US-PGPUB; USPAT; USOCR	OR	ON	2010/02/13 12:42
L21	27	((EDMUND) near2 (MUNGER)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2010/02/13 12:42
L22	75	((MICHAEL) near2 (WILLIAMSON)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2010/02/13 12:43
L23	1573	l19 or l20 or l21 or "l75"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/02/13 12:43
L24	250	l19 or l20 or l21 or l22	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/02/13 12:43
L25	33	l24 and (l1 or l2)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/02/13 12:44
L26	28	l24 and l3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/02/13 12:44


L27	23311	"726"/\$.cls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/02/13 12:51
L28	184	I27 and I3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/02/13 12:51
L29	91	I28 and I5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/02/13 12:51
L30	3	I29 and @ad<="19981030"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/02/13 12:51

EAST Search History (Interference)

<This search history is empty>

2/ 13/ 10 12:52:27 PM

C:\Documents and Settings\ klim\ My Documents\ EAST\ Workspaces\ 11685142.wsp

Search Notes 	Application/Control No. 11839987	Applicant(s)/Patent Under Reexamination LARSON ET AL.
	Examiner Krisna Lim	Art Unit 2453

SEARCHED			
Class	Subclass	Date	Examiner
709	225-229, 245	2/13/2010	kl
726	15	2/13/2010	kl

SEARCH NOTES		
Search Notes	Date	Examiner
EAST, Inventors	2/13/2010	kl

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner
709	227, 228	2/13/2010	kl

--	--

Subst. for form 1449/PTO SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Complete if Known		
				Application Number	11/839,987	
				Filing Date	August 16, 2007	
				First Named Inventor	Victor Larson	
				Art Unit	2453	
Examiner Name	LIM, Krisna					
Sheet	1	of	1	Docket Number	077580-0066 (VRNK-1CP2DVCN2)	

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Codez (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1019	US 7,461,334	12/02/08	Lu, et al.	
	A1020	US 7,353,841	04/08/08	Kono, et al.	
	A1021	US 7,188,175	03/06/07	McKeeth, James A.	
	A1022	US 7,167,904	01/23/07	Devarajan, et al.	
	A1023	US 7,039,713	05/02/06	Van Gunter, et al.	
	A1024	US 6,757,740	06/29/04	Parekh, et al.	
	A1025	US 6,752,166	06/22/04	Lull, et al.	
	A1026	US 6,687,746	02/03/04	Shuster, et al.	
	A1027	US 6,338,082	01/08/02	Schneider, Eric	
	A1028	US 6,333,272	12/25/01	McMillin, et al.	
	A1029	US 6,314,463	11/06/01	Abbott, et al.	
	A1030	US 6,298,341	10/02/01	Mann, et al.	
	A1031	US 6,262,987	07/17/01	Mogul, Jeffrey C.	
	A1032	US 6,199,112 ^{03/2001} 03/06/04	03/06/04	Wilson, Stephen K.	
	A1033	US 2,895,502	07/21/59	Garland Roper Charles, et al.	
	A1034	US 2001/0049741	12/06/01	Skene, et al.	

mmc
5-510

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes -Number +-Kind Codes (if known)	Publication Date MM-DD-YYYY	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.
	C1240	David Kosiur, "Building and Managing Virtual Private Networks" (1998)
	C1241	P. Mockapetris, "Domain Names - Implementation and Specification," Network Working Group, RFC 1035 (November 1987)
	C1242	Request for Inter Partes Reexamination of Patent No. 6,502,135, dated Nov. 25, 2009.
	C1243	Request for Inter Partes Reexamination of Patent No. 7,188,180, dated Nov. 25, 2009.

EXAMINER /Krisna Lim/	DATE CONSIDERED 02/13/2010
-----------------------	----------------------------

*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.
 BST99 1640184-1.077580.0066

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

Application Number	11839987	Filing Date	2007-08-16	Docket Number (if applicable)	077580-0066	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 _____

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

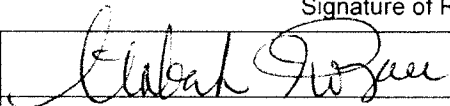
The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.

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		Date (YYYY-MM-DD)	04/01/2010
Name	Atabak R. Royae	Registration Number	59037

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

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

Subst. for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Application Number	11/839,987
				Filing Date	08/16/2007
				First Named Inventor	Victor Larson
				Art Unit	2453
				Examiner Name	Krisna Lim
				Docket Number	077580-0066

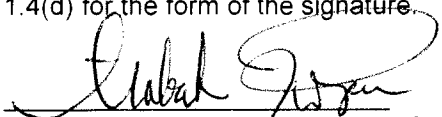
CERTIFICATION STATEMENT

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

- Information Disclosure Statement is being filed before the receipt of a first office action.
- Items contained in this Information Disclosure Statement were first cited in any communication from a foreign patent office in a counterpart foreign application.
- No item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned, after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of this Information Disclosure Statement
- The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of \$180.00, or further fees which may be due, to Deposit Account 50-1133.
- Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of \$810.00, or further fees which may be due, to Deposit Account 50-1133.
- None

SIGNATURE

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


 Atabak R. Royae, Reg. No.: 59,037
 McDermott Will & Emery LLP
 28 State Street
 Boston, MA 02108
 Tel. (617) 535-4000
 Fax (617) 535-3800

Date: 01/01/2010

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known

Application Number	11/839,987
Filing Date	08/16/2007
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Docket Number	077580-0066

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
	A1	5,764,906	06/1998	Edelstein et al.	
	A2	5,864,666	01/1999	Shrader, Theodore Jack London	
	A3	5,898,830	04/1999	Wesinger et al.	
	A4	6,052,788	04/2000	Wesinger et al.	
	A5	6,061,346	05/2000	Nordman, Mikael	
	A6	6,081,900	06/2000	Subramaniam et al.	
	A7	6,101,182	08/2000	Sistanizadeh et al.	
	A8	6,199,112	03/2001	Wilson, Stephen K.	
	A9	6,202,081	03/2001	Naudus, Stanley T.	
	A10	6,298,341	10/2001	Mann et al.	
	A11	6,262,987	07/2001	Mogul, Jeffrey C.	
	A12	6,314,463	11/2001	Abbott et al.	
	A13	6,338,082	01/2002	Schneider, Eric	
	A14	6,502,135	12/2002	Munger et al.	
	A15	6,557,037	04/2003	Provino, Joseph E.	
	A16	6,687,746	02/2004	Shuster et al.	
	A17	6,757,740	06/2004	Parkh et al.	
	A18	7,039,713	05/2006	Van Gunter et al.	
	A19	7,167,904	01/2007	Devarajan et al.	
	A20	7,188,175	03/2007	McKeeth, James A.	
	A21	7,461,334	12/2008	Lu et al.	
	A22	7,490,151	02/2009	Munger et al.	
	A23	7,493,403	02/2009	Shull 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
	B1	US2001/0049741	12/2001	Skene et al.	
	B2	US2004/0199493	10/2004	Ruiz et al.	
	B3	US2004/0199520	10/2004	Ruiz et al.	
	B4	US2004/0199608	10/2004	Rechterman et al.	
	B5	US2004/0199620	10/2004	Ruiz et al.	
	B6	US2007/0208869	09/2007	Adelman et al.	
	B7	US2007/0214284	09/2007	King et al.	

Subst. for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Application Number	11/839,987
				Filing Date	08/16/2007
				First Named Inventor	Victor Larson
				Art Unit	2453
				Examiner Name	Krisna Lim
				Docket Number	077580-0066

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
	B8	US2007/0266141	11/2007	Norton, Michael Anthony	
	B9	US2008/0235507	09/2008	Ishikawa et al.	

FOREIGN PATENT DOCUMENTS							
EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes-Number + -Kind Codes (if known)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No
	C1	JP04-363941	12/16/1992	Nippon Telegr & Teleph Corp		English Abstract	
	C2	JP09-018492	01/17/1997	Nippon Telegr & Teleph Corp		English Abstract	
	C3	JP10-070531	03/10/1998	Brother Ind Ltd.		English Abstract	
	C4	JP62-214744	9/21/1987	Hitachi Ltd.		English Abstract	

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	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)	
	D2	D.W. Davies and W.L. Price, edited by Tadahiro Uezono, "Network Security", Japan, Nikkei McGraw-Hill, December 5, 1958, First Edition, first copy, p. 102-108	
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.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 62-214744

(43)Date of publication of application : 21.09.1987

(51)Int.Cl. H04L 9/00

H04L 11/20

H04L 11/26

(21)Application number : 61-056812

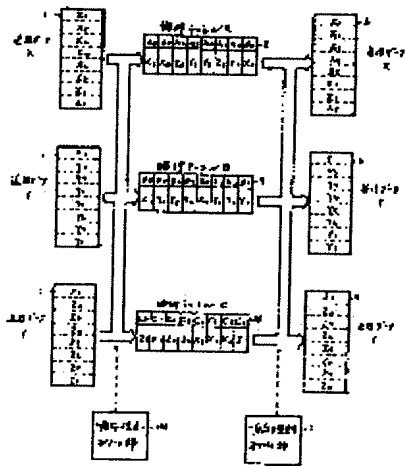
(71)Applicant : HITACHI LTD

(22)Date of filing : 17.03.1986

(72)Inventor : OOYA KAZUAKI

HIRAGA KATSUHISA

(54) PACKET TRANSMISSION SYSTEM



(57)Abstract:

PURPOSE: To prevent the leakage of data by providing a means controlling the order of packet by a prescribed definition to the reception and transmission side, deciding the logical channel of each packet in the order of sending at the transmission side and restoring the data string of the packet received from each logical channel at the reception side.

CONSTITUTION: Data X, Y, Z to be sent of data 1, 4, 7 are split at each packet, a transmission order rule control section 10 is used to share the packets into logical channels A, B, C of data 2, 5, 8. In this case, the sent order is changed according to the sequence restriction of the control section 10. Thus, the packet

data are sent in the entirely difference order from that of the packet data constituting the original data 1, 4, 7 to be sent. At the reception side, the packet data received from each logical channel (2, 5, 8) is rearranged by a reception side order rule control section 11 to obtain reception data X, Y, Z of data 3, 6, 7. Thus, the leakage of the data from the transmission line and the decoding are prevented.

Cited Document 1 (JP-A (Kokai) S62-214744)

The order of packet data in each logical channel of the present invention is different from those in logical channels 2, 5, and 8 of the conventional packet transmission system as shown in Fig. 5 in that correct information cannot be obtained at the receiver even if the data in one logical channel are aligned sequentially, as indicated by 2, 5, and 8 in Fig. 1. Therefore, at the receiver, it is necessary to realign the data received from each logical channel with reference to the same order rule as that used at the transmitter.

Fig. 2 shows an example of the order rule. When arranged in a table indicated by 12, this order rule forms a matrix in which 24 types of numerals from A1 to C8, configured by the combination of the logical channel numbers of A, B, and C, and the sequence numbers from 1 to 8, correspond to the packet data from X1 to Z8 obtained by dividing the corresponding transmission data X, Y, and Z.

Fig. 3 shows an example of processing at the transmitter. When the data to be transmitted via the logical channel A of 2 are selected from the transmission data X, Y, and Z of 1, 4, and 7, the order rule shown in the table 12 in Fig. 3 is used to send out the packets in the order of X₁, Y₂, Z₂, Y₆, Y₇, and Z₆ to the logical channel A. The same applies to the data to be transmitted via the logical channels B and C of 5 and 8.

Fig. 4 shows an example of processing at the receiver. For example, the data X₁, Y₂, Z₂, Y₆, Y₇, and Z₆ received from the logical channel A indicated by 2 are aligned in each position of the received data X, Y, and Z indicated by 3, 6, and 9 according to the order rule of the logical channel A as shown in table 12 of Fig. 3. The same processing is executed for the other logical channels to restore the received data X, Y, and Z.

⑨ 日本国特許庁(JP)

⑩ 特許出願公開

⑫ 公開特許公報(A)

昭62-214744

⑮ Int.Cl. ⁴	識別記号	庁内整理番号	⑬ 公開
H 04 L 9/00		B-7240-5K	昭和62年(1987)9月21日
11/20	1 0 2	A-7117-5K	
11/26		7117-5K	審査請求 未請求 発明の数 1 (全4頁)

⑭ 発明の名称 パケット伝送方式

⑯ 特 願 昭61-56812

⑰ 出 願 昭61(1986)3月17日

⑱ 発 明 者	大 家	万 明	秦野市堀山下1番地	株式会社日立製作所神奈川工場内
⑲ 発 明 者	平 賀	勝 久	秦野市堀山下1番地	株式会社日立製作所神奈川工場内
⑳ 出 願 人	株式会社日立製作所			東京都千代田区神田駿河台4丁目6番地
㉑ 代 理 人	弁理士	小川 勝男	外1名	

明 細 書

1. 発明の名称

パケット伝送方式

2. 特許請求の範囲

(1) 送信側と受信側において複数の論理チャネルを使用しデータをパケット分割して伝送するパケット伝送方式において、送信側と受信側にパケットの送信及び受信の順序を予め定めた定義に従って制御する順序規則制御手段を持ち、この順序規則制御手段により、送信側では受信する各パケットの論理チャネル及び送出順序を決定し、受信側では各論理チャネルから受信したパケットのデータ列の復元を行うことを特徴としたパケット伝送方式。

3. 発明の詳細な説明

(産業上の利用分野)

本発明はパケット伝送方式に係り、特に伝送内容の秘密を守るため、伝送路上でデータが第3者に漏れ、これが容易に解析されることを防ぐのに好適なパケット伝送方式に関する。

(従来技術)

パケット伝送方式の一つに、送信側と受信側において複数の論理チャネルを使用し、データをパケット分割して伝送する方式がある(CCITT, X.25勧告)。

第5図に従来のこの種パケット伝送方式を示す。1, 4, 7は送信しようとするデータX, Y, Zであり、これをそれぞれパケット分割し、2, 5, 8の論理チャネルA, B, Cを経由して各々のパケットデータを受信側へ送信する。受信側では、各論理チャネルごとに受信したパケットデータをシーケンス番号順に整列させ、3, 6, 9の受信データX, Y, Zを得る。

なお、秘密データ伝送に関連する公知文献としては、例えば特開昭60-54544号公報が挙げられる。

(発明が解決しようとする問題点)

従来技術においては、受信側において論理チャネル番号とパケットシーケンス番号により、パケットデータの識別を行うため、データを受信した

側では容易にパケットの解読ができ、データが第3者へ漏洩するという問題があった。

本発明の目的は、伝送しようとするデータの形式を加工することなく、データを構成するパケットをそれぞれ異った仮想的通信路を通して伝送することにより、伝送しようとするデータが伝送路上から漏れ容易に解読されることを防ぐためのパケット伝送方式を提供することにある。

〔問題点を解決するための手段〕

本発明は、伝送しようとするデータを、同一の論理チャンネルを過ぎずに、データを構成する複数のパケットをあらかじめ定めた規則により、いくつかの異った論理チャンネルを使用して分割伝送する。あらかじめ定めた規則とは伝送しようとする一定順序のパケットをどの順序でどの仮想的通信路に送出するかを決めた通信路ごとの順序規則を言う。パケットを送信する側では、伝送しようとするデータを構成する一連のパケットを上記規則に従って仮想的通信路に順次送出する。パケットを受信する側では、同様上記規則に従い、各仮

想的通信路より受信したパケットを整理させ元のデータ列を復元する。

〔作用〕

本発明は、データの漏洩を防止することを目的とし、伝送しようとするパケット列の順序及び伝送路に関してスクランプリングしようとするものである。従来のパケット伝送では、各パケットごとに持つ論理チャンネル番号及びシーケンス番号を用いて、送信側と受信側のデータ側の順序制御を行っているため、受信側では受信したパケットデータ列から得られる情報のみで容易に元のデータ列を復元させることが容易である。

本発明においては、送信側と受信側にあらかじめ定義した論理チャンネルとシーケンス番号から成る送信及び受信パケットの順序を変換するための順序規則を持ち、この順序情報と各パケットに持つ論理チャンネル番号とパケットシーケンス番号を用いて、元のデータ列を復元させる。従って順序規則を持たないものが受信しても解読はできない。

〔実施例〕

以下、本発明の一実施例について図面により説明する。

第1図に本発明のパケット伝送方式を示す。1, 4, 7の送信しようとするデータX, Y, Zをそれぞれパケット分割し、10の送信側順序規則制御部を用いて、それぞれのパケットを2, 5, 8の各論理チャンネルA, B, Cに振り分ける。この際、送出する順序も制御部10の順序規則に従って変化させる。従って、各論理チャンネル2, 5, 8上には、図示の如く、送出しようとする元のデータ1, 4, 7を構成するパケットデータとはまったく異った順序で、パケットデータが伝送されることになる。受信側では、2, 5, 8の各論理チャンネルより受信したパケットデータを、11の受信側順序規則制御部により整理し直し、3, 6, 7の受信データX, Y, Zを得る。

本発明における各論理チャンネル上のパケットデータの順序は、第5図に示す従来のパケット伝送方式の論理チャンネル2, 5, 8と異なり、第1図の2, 5, 8に示す様に1つの論理チャンネル内の

データを順に整理させても受信側では正しい情報を得ることができない。従って、受信側では、送信側と同じ順序規則を参照して、各論理チャンネルから受信したデータを再度整理させる必要がある。

第2図に順序規則の1例を示す。この順序規則例は、12に示すテーブル形式とした場合、A, B, Cの論理チャンネル番号と1から8のシーケンス番号との組み合わせによって構成されるA1からC8までの24種類の番号と、これに対応する送信データX, Y, Zを分割したX1からZ8のパケットデータを対応させたマトリックスとなる。

第3図に送信側の処理例を示す。1, 4, 7の送信データX, Y, Zより、2の論理チャンネルA経由で送信するデータを選択する場合、第3図のテーブル12に示した順序規則を用いて、論理チャンネルAに対して、X₁, Y₂, Z₃, Y₄, Y₅, Z₆の順序でパケットを送出する。5と8の論理チャンネルB, C経由で送信するデータも同様である。

第4図に受信側の処理例を示す。例えば、2に

示す論理チャネルAより受信したデータ、 $X_1, Y_2, Z_3, Y_4, Y_7, Z_8$ は、第3図のテーブル12で示した論理チャネルAの順序規則に従い、3, 6, 9に示される受信データX, Y, Zそれぞれの位相に整列される。他の論理チャネルについても同様の処理を行い、受信データX, Y, Zを復元させる。

なお、順序規則は、テーブル形式で定義する方式のほかに、計算式で定義する方式が考えられる。
〔発明の効果〕

本発明によれば、あらかじめ定められた順序規則を知っている場合のみ、パケットデータの正しい送受信が行える。従って、順序規則を知らされていない第三者は正しい受信を行うことが出来ず、データの機密を守る上で効果がある。また、本発明においては、複数の論理チャネルを使用するため、各論理チャネルを物理的に別々の回線に分割して配置することが出来、この時には物理的に別々の回線を同時に接続して受信する必要があるため、データの漏洩防止にさらに効果がある。

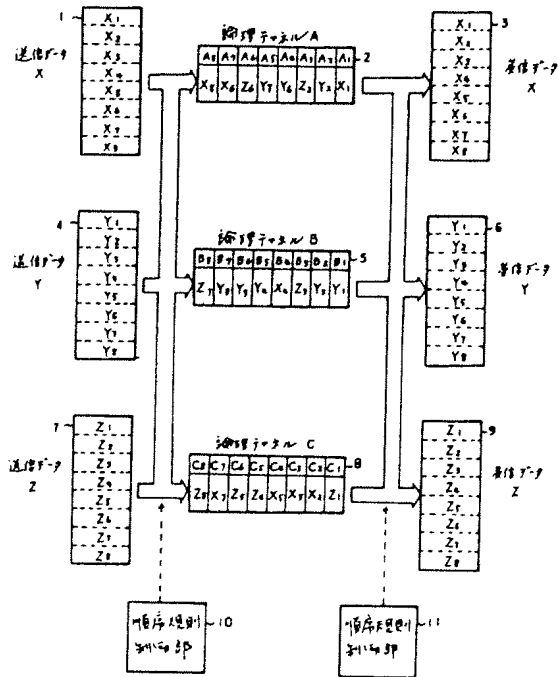
4. 図面の簡単な説明

第1図は本発明のパケット伝送方式を説明する図、第2図は本発明で用いる順序規則の一例を示す図、第3図は本発明による送信側の処理例を示す図、第4図は本発明による受信側の処理例を示す図、第5図は従来のパケット伝送方式を説明する図である。

- 1, 4, 7...送信データ、
- 3, 6, 9...受信データ、
- 2, 5, 8...論理チャネル、
- 10...送信側順序規則制御部、
- 11...受信側順序規則制御部。

代理人弁理士 小川 勝 男

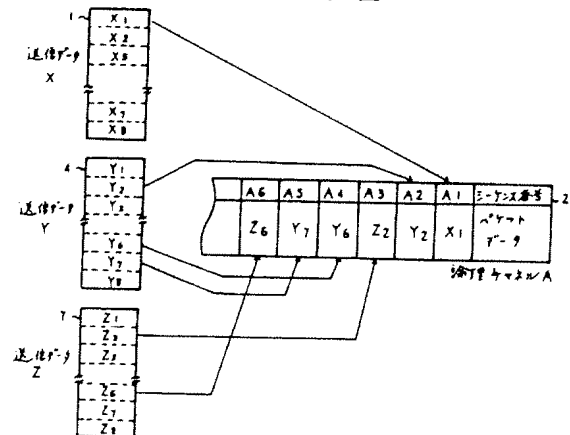
第1図



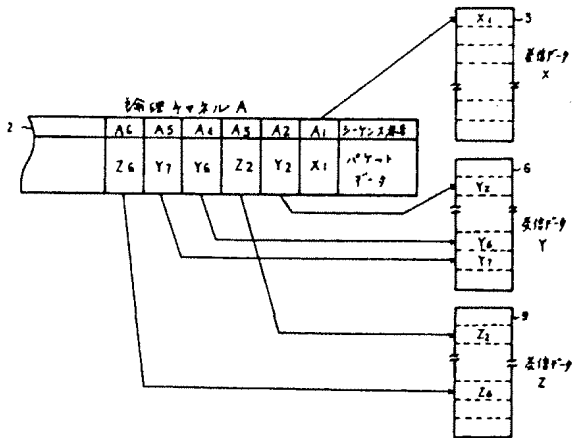
第2図

送信側	1	2	3	4	5	6	7	8	12
A	X ₁	Y ₂	Z ₃	Y ₆	Y ₇	Z ₈	X ₆	X ₈	
B	Y ₁	Y ₃	Z ₃	X ₄	Y ₄	Y ₅	Y ₈	Z ₇	
C	Z ₁	X ₂	X ₃	X ₅	Z ₄	Z ₅	X ₇	Z ₈	

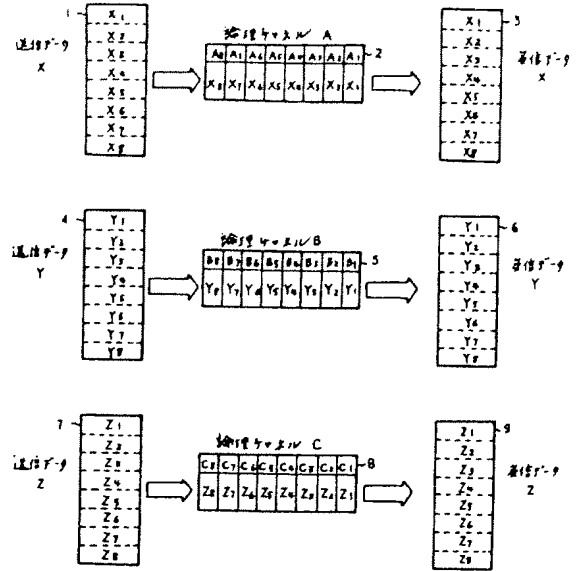
第3図



第4図



第5図



PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-070531

(43)Date of publication of application : 10.03.1998

(51)Int.Cl. H04L 12/22
G06F 13/00
H04K 1/00

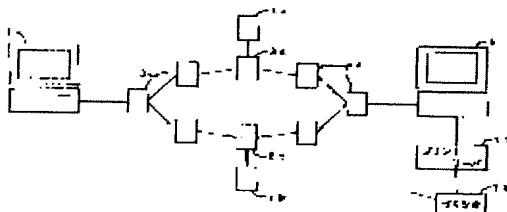
(21)Application number : 08-223898 (71)Applicant : BROTHER IND LTD
(22)Date of filing : 26.08.1996 (72)Inventor : SUZUKI MASASHI
MATSUDA KAZUHIKO
SAGOU AKIRA
KONDO HIROMOTO
YASUI TSUNEO

(54) DATA COMMUNICATION SYSTEM AND RECEIVER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a data communication system capable of satisfactorily preventing the leakage of data to be communicated.

SOLUTION: A personal computer 1 bi-sects data to be transmitted, adds transmission source data and transmission time data to the respective bisected data and transmits respective data to different servers 7a and 7b through different communication routes. Then the respective servers 7a and 7b transmit each received data to a server 5 through the communication route. The server 5 judges whether or not the transmission source data and transmission time



data of the received data is matched with those of the already received data, and at the time they are matched, the received data is combined with the already received to obtain data before bisecting.

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1]A data communication system provided with a sending set characterized by comprising the following which transmits data, and a receiving set which receives the above-mentioned data transmitted from this sending set.

A data dividing means into which it has two or more repeating installation which relays separately the above-mentioned data transmitted to the above-mentioned receiving set via a different communication path from the above-mentioned sending set, and the above-mentioned sending set divides the above-mentioned data at plurality.

An identification data grant means to give identification data which matches the data with each data divided in this data dividing means mutually.

A data sending means which transmits each data in which the above-mentioned identification data was given to the mutually different above-mentioned repeating installation.

A data-coupling means to combine the data which have and have identification data in which the above-mentioned receiving set corresponds mutually among each data received in a data receiving means which receives data separately from each above-mentioned repeating installation, and this data receiving means.

[Claim 2]The data communication system according to claim 1, wherein the above-mentioned identification data contains transmission source data showing common transmitting origin, and transmission time data showing having been mostly transmitted to identical time.

[Claim 3]The data communication system according to claim 1 or 2, wherein the above-mentioned identification data contains a serial number which has numerals common to at least a part.

[Claim 4]A receiving set comprising:

A data receiving means which receives data separately via mutually different repeating

installation.

A data-coupling means to combine the data which have the above-mentioned identification data mutually corresponding among data received from each data received in this data receiving means in an identification data extraction means to extract predetermined identification data, and the above-mentioned data receiving means.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the data communication system provided with the sending set which transmits data, and the receiving set which receives the data transmitted from the sending set, and a receiving set applicable to the data communication system.

[0002]

[Description of the Prior Art] Conventionally, in this kind of data communication system, receiving the data which transmitted data from the sending set via the telephone line and the cable, and was transmitted from that sending set with a receiving set is performed. Performing such data communications through the Internet is also considered in recent years.

[0003]

[Problem(s) to be Solved by the Invention] However, in this kind of data communication system, since the whole data was transmitted and received via a telephone line, a cable, etc., the data which spreads a telephone line, a cable, etc. may have been monitored by the 3rd person. For this reason, it was difficult to prevent disclosure of the data which communicates. Especially the Internet was easy to access and it was much more difficult to prevent disclosure of data.

[0004] Then, the invention according to claim 3 was made [that especially the invention according to claim 2 simplifies composition further for the purpose of the invention according to claim 1 to 3 providing the data communication system which can prevent disclosure of the data which communicates good, and] for the purpose of performing the reconstitution of data much more correctly. The invention according to claim 4 was made for the purpose of providing a receiving set applicable to the data communication system.

[0005]

[The means for solving a technical problem and an effect of the invention] The invention according to claim 1 made since the above-mentioned purpose was attained, In the data communication system provided with the sending set which transmits data, and the receiving set which receives the above-mentioned data transmitted from this sending set, Have two or more repeating installation which relays separately the above-mentioned data transmitted to the above-mentioned receiving set via a different communication path from the above-mentioned sending set, and. The data dividing means to which the above-mentioned sending set divides the above-mentioned data into plurality, and an identification data grant means to give the identification data in which the data is mutually matched with each data in which it was divided in this data dividing means, The data sending means which transmits each data in which the above-mentioned identification data was given to the mutually different above-mentioned repeating installation, It **** and is characterized by having a data-coupling means to combine the data which have identification data in which the above-mentioned receiving set corresponds mutually among each data received in the data receiving means which receives data separately from each above-mentioned repeating installation, and this data receiving means.

[0006]In this invention constituted in this way, a sending set divides data into plurality by a data dividing means, and gives the identification data which matches data with the data of each which was divided mutually by an identification data grant means. A sending set transmits each data in which the above-mentioned identification data was given to mutually different repeating installation by a data sending means. Then, each repeating installation relays each data separately via a mutually different communication path, and a receiving set receives each above-mentioned data separately from each repeating installation by a data receiving means. Then, a receiving set combines the data which have identification data mutually corresponding among each received data by a data-coupling means.

[0007]For this reason, data combined by a data-coupling means of a receiving set is in agreement with data before division by a data dividing means of a sending set. That is, it means that data before division was transmitted even to a receiving set. Data by which each above-mentioned communication path is spread via repeating installation is data after division by ***** and a data dividing means. For this reason, even if data by which a communication path is spread is monitored, that data will not be in agreement with data before division.

[0008]Therefore, in this invention, disclosure of data which communicates can be prevented good. As a communication path, a telephone line, the Internet besides a cable,

etc. are applicable, and also when it is any, disclosure of data can be prevented good. In addition to the composition according to claim 1, the invention according to claim 2 is characterized by the above-mentioned identification data containing transmission source data showing common transmitting origin, and transmission time data showing having been mostly transmitted to identical time.

[0009]That is, data after the above-mentioned division is usually transmitted to the almost same time (a difference is less than 1 minute) from the same sending set. So, in this invention, transmission source data which expresses common transmitting origin to the above-mentioned identification data, and transmission time data showing having been mostly transmitted to identical time are included. For this reason, in a receiving set, data can be combined easily and it can restore. A common sending set is also equipped with a function which gives transmission source data and transmission time data in many cases. Therefore, when this invention is applied to such a sending set, even if it does not provide composition special as an identification data grant means, the above-mentioned sending set can be realized.

[0010]Therefore, in addition to the effect according to claim 1, in this invention, an effect that it can simplify further produces composition of a sending set. The invention according to claim 3 is characterized by the above-mentioned identification data containing a serial number which has numerals common to at least a part in addition to the composition according to claim 1 or 2.

[0011]In this invention constituted in this way, data after division is matched using a serial number which has common numerals at least in part. For this reason, the data after division can be matched very correctly. For example, when each data after division is long and transmission time of each data shifts substantially, each data can be matched good.

[0012]Therefore, in addition to the effect of the invention according to claim 1 or 2, in this invention, an effect that it can restore much more correctly produces data after division. The receiving set according to claim 4 is provided with the following.

A data receiving means which receives data separately via mutually different repeating installation.

An identification data extraction means to extract predetermined identification data from each data received in this data receiving means.

A data-coupling means to combine the data which have the above-mentioned identification data mutually corresponding among data received in the above-mentioned data receiving means.

[0013]With this invention constituted in this way, a data receiving means receives data separately via mutually different repeating installation, and an identification data extraction means extracts predetermined identification data from each received data. Then, a data-coupling means combines the data which have identification data mutually corresponding among data received in a data receiving means.

[0014]For this reason, this invention is applicable good as a receiving set in the data communication system according to any one of claims 1 to 3. the above-mentioned identification data may contain transmission source data showing common transmitting origin, and transmission time data showing having been mostly transmitted to identical time, may contain a serial number which boils a part at least and has common numerals, and may be a thing of other gestalten.

[0015]

[Embodiment of the Invention]Next, an embodiment of the invention is described with a drawing. Drawing 1 is an outline lineblock diagram showing the data communication system which applied this invention. This embodiment applies this invention to the network print system using the Internet.

[0016]As shown in drawing 1, the personal computer (henceforth a personal computer) 1 of the users as a sending set is connected to the server 5 as a receiving set by the side of a print service station via the Internet which connects many providers 3. For this reason, if data is transmitted towards the server 5 from the personal computer 1, that data will be spread via [the adjoining provider 3] one by one. The data which communicates the Internet top is once memorized to the two providers 3a and 3b who exist on a different communication path, and the servers 7a and 7b as repeating installation which changes an address (address of a transmission destination) and transmits are connected to them.

[0017]The personal computer 1 and the servers 5, 7a, and 7b are all the computers of the common knowledge provided with the external memory or the modem for communication besides CPU, ROM, and RAM, and the printer 13 is further connected to the server 5 via the print server 11. This system is for transmitting image data etc. to the server 5 of a print service station (printer) from users' (customer) personal computer 1, and performing image formation with the printer 13. The servers 5, 7a, and 7b may be FTP (file transfer protocol) servers, or may be mail servers.

[0018]Next, processing of the personal computer 1 in this system and the servers 5, 7a, and 7b is explained using drawing 2 - the flow chart of four. Users' personal computer 1 will perform processing of drawing 2, if transmission of data is directed via the keyboard etc. which are not illustrated. If processing is started as shown in drawing 2,

the data first transmitted in S1 will be read, and the data will be divided into two by S3 continuing. The 1st data after division is transmitted to the 1st address corresponding to the server 7a, by S7, the 2nd data after division is transmitted to the 2nd address corresponding to the server 7b, and processing is ended S5 continuing. In transmission of the data in S5 and S7, the transmission source data showing the address of the personal computer 1 which is a transmitting agency, and the transmission time data showing the transmission time are given to the data to transmit. Since this processing is common knowledge, it is not explained in full detail here. It is good also considering which of the data after division as the 1st at S5 and S7.

[0019]On the other hand, the server 7a carries out repeat execution of the processing shown in drawing 3. The server 7b also carries out repeat execution of the same processing. As shown in drawing 3, when processing was started, and it judges whether data was received or not and receives in S11 (S11:YES), it shifts to S13. The received data is stored in a predetermined memory by the routine of the common knowledge which is not illustrated. In S13, the received data is transmitted to the prescribed address corresponding to the server 5, and it shifts to S11. When data is not received (S11:NO), it stands by in S11 as it is.

[0020]For this reason, if the data after the personal computer 1 dividing is transmitted to the servers 7a and 7b by processing of drawing 2 (S5, S7), by processing of drawing 3, the servers 7a and 7b will receive each data after division separately (S11:YES), and will transmit that data to the server 5 (S13). That is, the data after division is transmitted to the server 5 via a different communication path.

[0021]Next, drawing 4 is a flow chart showing the processing in which the server 5 carries out repeat execution. If processing is started, when it judges whether data was received or not and receives in S21 (S21:YES), it will shift to S23. The received data is stored in a predetermined memory by the routine of the common knowledge which is not illustrated. In S23, the transmission source data given to the data judges whether a match has a match, i.e., the address of a transmitting agency, in the data which already receives and is stored in the memory. The data whose transmission time which shifts to S25 and transmission time data expresses in the already received data if there are data received in S21 and data whose address of a transmitting agency corresponds (S23:YES) corresponds mostly judges whether it is in it.

[0022]When an affirmative judgment is carried out by S25, the data received in S21 and the corresponding data which already received and was stored in the memory are the data continuously transmitted by S5 of drawing 2, and S7. Then, the data after combination is sent to the print server 11 in S29 which combines two data in S27 and

continues in this case (S25:YES), and it returns to S21. Then, image formation with the printer 13 is performed based on the data after combination, i.e., the data read in S1 of drawing 2. On the other hand, when a negative judgment is carried out by SS21, S23, or 25, nothing is done but it returns to S21 as it is.

[0023]Thus, in this system, it can restore by the server 5 and image formation of the data transmitted via a communication path which divides with the personal computer 1 and is different can be carried out with the printer 13. The data spread via each provider 3 is data after division, respectively. For this reason, even if the data spread via each provider 3 is monitored, that data will not be in agreement with the data before division. Therefore, in this system, disclosure of the data which communicates can be prevented good. In this system, the data which should be combined in S27 is identified with transmission source data and transmission time data. The common personal computer is also equipped with the function which gives transmission source data and transmission time data in many cases. In this system, since such a general function is used, processing can be simplified further.

[0024]Next, other embodiments of this invention are described using drawing 5 - the flow chart of seven. In this embodiment, since only processing of each part differs from the above-mentioned embodiment, the numerals used by drawing 2 are used as it is. In drawing 5 -7, the same numerals are given to drawing 2 - the same processing as four, and detailed explanation of processing is omitted to them.

[0025]Drawing 5 is a flow chart showing the processing which the personal computer 1 performs, when transmission of data is directed. After reading the data to transmit (S1) and dividing the data into two if processing is started as shown in drawing 5 (S3), it shifts to S31. In S31, a serial number is generated using a random number etc. from current time. As a serial number, the thing containing numerals other than numbers, such as the alphabet, may be adopted. In S33 continuing, "1" of the serial number and a number is given to the 1st data, and "2" of the above-mentioned serial number and a number is given to the 2nd data in S35. Then, each data after the division to which the serial number etc. were given is transmitted to the 1st and 2nd addresses (it corresponds to the servers 7a and 7b), and processing is ended (S5, S7).

[0026]Drawing 6 is a flow chart showing the processing in which the servers 7a and 7b carry out repeat execution. If data is received (S11:YES), it will shift to S41, and it is judged whether the serial number is given to the data. When given (S41:YES), it shifts to S13, and data is transmitted to the prescribed address corresponding to the server 5, and it shifts to S11. When data is not received (S11:NO), and when the serial number is not given (S41:NO), it shifts to S11 as it is. That is, since it is not the data transmitted

by S5 of drawing 5, and S7 when the serial number is not given, other routines which are not illustrated perform the usual processing as the servers 7a and 7b.

[0027]Drawing 7 is a flow chart showing the processing in which the server 5 carries out repeat execution. In this processing, if data is received (S21: YES), it will shift to S51, and it is judged whether the serial number is given to that data. It is judged whether there are what was given to the data, and a thing which has the same serial number in the data which shifts to S53 when given (S51: YES), already receives, and is stored in the memory.

[0028]When an affirmative judgment is carried out by S53, the data received in S21 and the corresponding data which already received and was stored in the memory are the data continuously transmitted by S5 of drawing 5, and S7. Then, two data is combined in this case (S27), and it sends to the print server 11 (S29). Then, image formation with the printer 13 is performed based on the data after combination. On the other hand, when a negative judgment is carried out by S21, S51, or S53, nothing is done but it returns to S21 as it is.

[0029]When this embodiment also divides data and makes a different communication path spread like the above-mentioned embodiment, disclosure of data can be prevented good. In this system, the data after division is matched using the serial number. For this reason, data can be restored much more correctly. For example, when each data after division is long and the transmission time of each data shifts substantially (i.e., when S5 of drawing 5 and the interval of S7 become large etc.), each data is matched good. When there is no serial number in data (S41: NO), the servers 7a and 7b perform the usual processing. For this reason, it is not necessary to extend the servers 7a and 7b for the above-mentioned processing.

[0030]The processing which gives the transmission source data and transmission time data in S5 and S7 in each above-mentioned embodiment, And in processing of S33 and S35, processing of S3 for an identification data grant means to a data dividing means. In transmitting processing of the data in S5 and S7, processing of S21 to a data sending means to a data receiving means. The processing which extracts transmission source data [in / to a data-coupling means / in processing of S27 / S23, S25, S51, and S53], transmission time data, or a serial number is equivalent to an identification data extraction means, respectively.

[0031]This invention is not limited to the above-mentioned embodiment at all, and can be carried out with various gestalten in the range which does not deviate from the gist of this invention. For example, this invention is applicable to the data communication system using various communication paths, such as a telephone line, a cable, radio

besides using the Internet a data communication system. However, the Internet is very easy to access. Therefore, when it applies to the data communication system using the Internet like the above-mentioned embodiment, the effect of the leakage control of the data based on this invention becomes much more remarkable.

[0032]Although this invention is applied to the server 5 of a receiver in the above-mentioned embodiment to the network print system which connected the printer 13, in addition to this, this invention is applicable to various data communication systems. For example, it is applicable also to the system which only transmits and receives data. In this case, what is necessary is just to omit processing (drawing 4, drawing 7) of the five serverS29.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is an outline lineblock diagram showing the data communication system which applied this invention.

[Drawing 2]It is a flow chart showing processing of the transmitting side personal computer of the system.

[Drawing 3]It is a flow chart showing processing of the server for relay of the system.

[Drawing 4]It is a flow chart showing processing of the receiver server of the system.

[Drawing 5]It is a flow chart showing other gestalten of processing of the above-mentioned transmitting side personal computer.

[Drawing 6]It is a flow chart showing other gestalten of processing of the above-mentioned server for relay.

[Drawing 7]It is a flow chart showing other gestalten of processing of the above-mentioned receiver server.

[Description of Notations]

1 -- Personal computer 3 -- Provider 5, 7a, 7b -- Server

11 -- Print server 13 -- Printer

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-70531

(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
H 0 4 L 12/22		9744-5K	H 0 4 L 11/26	
G 0 6 F 13/00	3 5 1		G 0 6 F 13/00	3 5 1 A
H 0 4 K 1/00			H 0 4 K 1/00	Z

審査請求 未請求 請求項の数 4 O L (全 7 頁)

(21) 出願番号	特願平8-223898	(71) 出願人	000005267 ブラザー工業株式会社 愛知県名古屋市瑞穂区苗代町15番1号
(22) 出願日	平成8年(1996) 8月26日	(72) 発明者	鈴木 正史 愛知県名古屋市瑞穂区苗代町15番1号 ブラザー工業株式会社内
		(72) 発明者	松田 和彦 愛知県名古屋市瑞穂区苗代町15番1号 ブラザー工業株式会社内
		(72) 発明者	佐郷 朗 愛知県名古屋市瑞穂区苗代町15番1号 ブラザー工業株式会社内
		(74) 代理人	弁理士 足立 勉

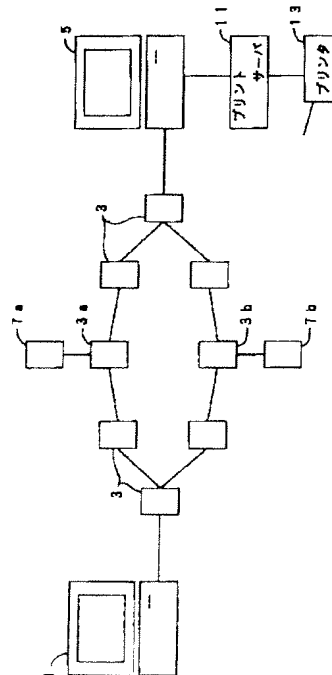
最終頁に続く

(54) 【発明の名称】 データ通信システムおよび受信装置

(57) 【要約】

【課題】 通信されるデータの漏洩を良好に防止できるデータ通信システムを提供することである。

【解決手段】 パソコン1によって、送信するデータを二つに分割し、その分割した各データにそれぞれ送信元データや送信時刻データを付して、その各データを異なる通信経路を介して別々のサーバ7 a、7 bに送信する。そして、各サーバ7 a、7 bは、受信した各データを異なる通信経路を介してサーバ5に送信する。サーバ5は、受信したデータと、既に受信しているデータとについて、前記送信元データや送信時刻データが一致するか否かを判断し、一致した場合は前記受信したデータと既に受信しているデータとを結合して分割前のデータにさせる。



【特許請求の範囲】

【請求項1】 データを送信する送信装置と、
 該送信装置から送信された上記データを受信する受信装置と、
 を備えたデータ通信システムにおいて、
 上記送信装置から上記受信装置へ送信される上記データを、異なる通信経路を介して個々に中継する複数の中継装置を備えると共に、
 上記送信装置が、
 上記データを複数に分割するデータ分割手段と、
 該データ分割手段にて分割された個々のデータに、そのデータ同士を互いに対応付ける識別データを付与する識別データ付与手段と、
 上記識別データが付与された各データを、互いに異なる上記中継装置へ送信するデータ送信手段と、
 を有し、
 上記受信装置が、
 上記各中継装置から個々にデータを受信するデータ受信手段と、
 該データ受信手段にて受信した各データの内、互いに対応する識別データを有するデータ同士を結合するデータ結合手段と、
 を有することを特徴とするデータ通信システム。

【請求項2】 上記識別データが、共通の送信元を表す送信元データと、ほぼ同一時刻に送信されたことを表す送信時刻データとを含むことを特徴とする請求項1記載のデータ通信システム。

【請求項3】 上記識別データが、少なくとも一部分に共通の符号を有するシリアルナンバーを含むことを特徴とする請求項1または2記載のデータ通信システム。

【請求項4】 互いに異なる中継装置を介して個々にデータを受信するデータ受信手段と、
 該データ受信手段にて受信した各データから、所定の識別データを抽出する識別データ抽出手段と、
 上記データ受信手段にて受信したデータの内、互いに対応する上記識別データを有するデータ同士を結合するデータ結合手段と、
 を備えたことを特徴とする受信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、データを送信する送信装置と、その送信装置から送信されたデータを受信する受信装置とを備えたデータ通信システム、およびそのデータ通信システムに適用可能な受信装置に関する。

【0002】

【従来の技術】従来、この種のデータ通信システムでは、電話回線やケーブルを介して送信装置からデータを送信し、その送信装置から送信されたデータを受信装置にて受信することが行われている。また、近年、インターネットを通じてこのようなデータ通信を行うことも考

えられている。

【0003】

【発明が解決しようとする課題】ところが、この種のデータ通信システムでは、電話回線やケーブル等を介してデータ全体が送受信されるので、電話回線やケーブル等を伝搬するデータが第三者によって傍受される可能性があった。このため、通信されるデータの漏洩を防止するのが困難であった。特に、インターネットはアクセスが容易であり、データの漏洩を防止することが一層困難であった。

【0004】そこで、請求項1～3記載の発明は、通信されるデータの漏洩を良好に防止できるデータ通信システムを提供することを目的とし、特に、請求項2記載の発明は構成を一層簡略化することを、請求項3記載の発明はデータの復元を一層正確に行うことを目的としてなされた。また、請求項4記載の発明は、そのデータ通信システムに適用可能な受信装置を提供することを目的としてなされた。

【0005】

【課題を解決するための手段および発明の効果】上記目的を達するためになされた請求項1記載の発明は、データを送信する送信装置と、該送信装置から送信された上記データを受信する受信装置と、を備えたデータ通信システムにおいて、上記送信装置から上記受信装置へ送信される上記データを、異なる通信経路を介して個々に中継する複数の中継装置を備えると共に、上記送信装置が、上記データを複数に分割するデータ分割手段と、該データ分割手段にて分割された個々のデータに、そのデータ同士を互いに対応付ける識別データを付与する識別データ付与手段と、上記識別データが付与された各データを、互いに異なる上記中継装置へ送信するデータ送信手段と、を有し、上記受信装置が、上記各中継装置から個々にデータを受信するデータ受信手段と、該データ受信手段にて受信した各データの内、互いに対応する識別データを有するデータ同士を結合するデータ結合手段と、を有することを特徴としている。

【0006】このように構成された本発明では、送信装置は、データ分割手段によりデータを複数に分割し、その分割された個々のデータに、データ同士を互いに対応付ける識別データを、識別データ付与手段によって付与する。更に、送信装置は、データ送信手段により、上記識別データが付与された各データを互いに異なる中継装置に送信する。すると、各中継装置は、各データを互いに異なる通信経路を介して個々に中継し、受信装置は、データ受信手段により、上記各データを各中継装置から個々に受信する。続いて、受信装置は、データ結合手段により、受信した各データの内、互いに対応する識別データを有するデータ同士を結合する。

【0007】このため、受信装置のデータ結合手段により結合されたデータは、送信装置のデータ分割手段によ

る分割前のデータと一致する。すなわち、分割前のデータが受信装置まで送信されたことになる。また、中継装置を介して上記各通信経路を伝搬されるデータは、それぞれ、データ分割手段による分割後のデータである。このため、通信経路を伝搬されるデータが仮に傍受されても、そのデータは分割前のデータとは一致しない。

【0008】従って、本発明では、通信されるデータの漏洩を良好に防止することができる。なお、通信経路としては、電話回線やケーブルの他、インターネット等も適用することができ、いずれの場合もデータの漏洩を良好に防止することができる。請求項2記載の発明は、請求項1記載の構成に加え、上記識別データが、共通の送信元を表す送信元データと、ほぼ同一時刻に送信されたことを表す送信時刻データとを含むことを特徴としている。

【0009】すなわち、上記分割後のデータは、通常、同じ送信装置からほぼ同一時刻（例えば差が1分未満）に送信される。そこで、本発明では、上記識別データに、共通の送信元を表す送信元データと、ほぼ同一時刻に送信されたことを表す送信時刻データとを含めてい

る。このため、受信装置では、データを容易に結合して復元することができる。また、送信元データおよび送信時刻データを付与する機能は、一般の送信装置にも備えられている場合が多い。よって、このような送信装置に本発明を適用した場合、識別データ付与手段として特別な構成を設けなくても上記送信装置を実現することができる。

【0010】従って、本発明では、請求項1記載の効果に加えて、送信装置の構成を一層簡略化することができるといった効果が生じる。請求項3記載の発明は、請求項1または2記載の構成に加え、上記識別データが、少なくとも一部分に共通の符号を有するシリアルナンバーを含むことを特徴としている。

【0011】このように構成された本発明では、分割後のデータを少なくとも一部に共通の符号を有するシリアルナンバーを用いて対応付けている。このため、分割後のデータ同士をきわめて正確に対応付けることができる。例えば、分割後の各データが長くて各データの送信時刻が大幅にずれたときなどにも、各データを良好に対応付けることができる。

【0012】従って、本発明では、請求項1または2記載の発明の効果に加えて、分割後のデータを一層正確に復元することができるといった効果が生じる。請求項4記載の受信装置は、互いに異なる中継装置を介して個々にデータを受信するデータ受信手段と、該データ受信手段にて受信した各データから、所定の識別データを抽出する識別データ抽出手段と、上記データ受信手段にて受信したデータの内、互いに対応する上記識別データを有するデータ同士を結合するデータ結合手段と、を備えたことを特徴としている。

【0013】このように構成された本発明では、データ受信手段は互いに異なる中継装置を介して個々にデータを受信し、識別データ抽出手段は、受信した各データから所定の識別データを抽出する。すると、データ結合手段は、データ受信手段にて受信したデータの内、互いに対応する識別データを有するデータ同士を結合する。

【0014】このため、本発明は、請求項1～3のいずれかに記載のデータ通信システムにおける受信装置として、良好に適用することができる。なお、上記識別データは、共通の送信元を表す送信元データと、ほぼ同一時刻に送信されたことを表す送信時刻データとを含むものであってもよく、少なくとも一部分に共通の符号を有するシリアルナンバーを含むものであってもよく、その他の形態のものであってもよい。

【0015】

【発明の実施の形態】次に、本発明の実施の形態を図面と共に説明する。図1は本発明を適用したデータ通信システムを表す概略構成図である。なお、本実施の形態は、インターネットを利用したネットワークプリントシステムに本発明を適用したものである。

【0016】図1に示すように、送信装置としてのユーザー側のパーソナルコンピュータ（以下パソコンという）1は、多数のプロバイダ3を接続してなるインターネットを介してプリントサービスステーション側の受信装置としてのサーバ5に接続されている。このため、パソコン1からサーバ5に向けてデータを送信すると、そのデータは隣接するプロバイダ3を順次経由して伝搬される。また、異なる通信経路上に存在する二つのプロバイダ3a、3bには、インターネット上を通信されるデータを一旦記憶し、宛名（送信先のアドレス）を変えて送信する中継装置としてのサーバ7a、7bが接続されている。

【0017】なお、パソコン1およびサーバ5、7a、7bは、いずれも、CPU、ROM、RAMの他、外付けのメモリや通信用のモデムを備えた周知のコンピュータで、サーバ5には、更に、プリントサーバ11を介してプリンタ13が接続されている。本システムは、ユーザー（顧客）側のパソコン1からプリントサービスステーション（印刷業者）のサーバ5へ画像データ等を送信して、プリンタ13による画像形成を行うためのものである。また、サーバ5、7a、7bは、FTP（ファイル・トランスファー・プロトコル）サーバであっても、メールサーバであってもよい。

【0018】次に、本システムにおけるパソコン1およびサーバ5、7a、7bの処理を、図2～4のフローチャートを用いて説明する。ユーザー側のパソコン1は、図示しないキーボード等を介してデータの送信が指示されると、図2の処理を実行する。図2に示すように、処理を開始すると、まずS1にて送信するデータを読み込み、続くS3でそのデータを二つに分割する。続くS5

では、分割後の1つ目のデータをサーバ7 aに対応する第1アドレスへ送信し、S 7では、分割後の2つ目のデータをサーバ7 bに対応する第2アドレスへ送信して処理を終了する。なお、S 5、S 7におけるデータの送信に当たっては、送信元であるパソコン1のアドレスを表す送信元データと、その送信時刻を表す送信時刻データとが、送信するデータに付与される。この処理は周知であるのでここでは詳述しない。また、S 5、S 7では分割後のデータのどちらを1つ目としてもよい。

【0019】一方、サーバ7 aは図3に示す処理を繰り返し実行する。なお、サーバ7 bも同様の処理を繰り返し実行する。図3に示すように、処理を開始すると、S 11にてデータを受信したか否かを判断し、受信した場合(S 11: YES)はS 13へ移行する。なお、受信したデータは、図示しない周知のルーチンにより所定のメモリに格納される。S 13では、受信したデータをサーバ5に対応する所定アドレスへ送信してS 11へ移行する。また、データを受信していない場合(S 11: NO)は、そのままS 11にて待機する。

【0020】このため、図2の処理により、パソコン1が分割後のデータをサーバ7 a、7 bに送信すると(S 5、S 7)、図3の処理により、サーバ7 a、7 bは分割後の各データを個々に受信し(S 11: YES)、そのデータをサーバ5に送信する(S 13)。すなわち、分割後のデータが異なる通信経路を介してサーバ5に送信される。

【0021】次に、図4はサーバ5が繰り返し実行する処理を表すフローチャートである。処理を開始すると、S 21にてデータを受信したか否かを判断し、受信した場合(S 21: YES)はS 23へ移行する。なお、受信したデータは、図示しない周知のルーチンにより所定のメモリに格納される。S 23では、既に受信してメモリに格納されているデータの中で、そのデータに付与された送信元データが一致するもの、すなわち、送信元のアドレスが一致するものがあるか否かを判断する。既に受信したデータの中で、S 21にて受信したデータと送信元のアドレスが一致するデータがあれば(S 23: YES)、S 25へ移行し、送信時刻データが表す送信時刻がほぼ一致するデータが、その中にあるか否かを判断する。

【0022】S 25で肯定判断した場合、S 21にて受信したデータと、既に受信してメモリに格納されていた該当データとは、図2のS 5、S 7で連続して送信されたデータである。そこで、この場合(S 25: YES)、S 27にて二つのデータを結合し、続くS 29にて結合後のデータをプリントサーバ11へ送付してS 21へ戻る。すると、結合後のデータ、すなわち、図2のS 1にて読み込まれたデータに基づき、プリンタ13による画像形成が実行される。一方、S 21、S 23、S 25のいずれかで否定判断した場合は、何もせずそのま

まS 21へ戻る。

【0023】このように、本システムでは、パソコン1により分割して異なる通信経路を介して送信されたデータを、サーバ5にて復元し、プリンタ13にて画像形成することができる。また、各プロバイダ3を介して伝搬されるデータは、それぞれ分割後のデータである。このため、各プロバイダ3を介して伝搬されるデータが仮に傍受されても、そのデータは分割前のデータとは一致しない。従って、本システムでは、通信されるデータの漏洩を良好に防止することができる。更に、本システムでは、S 27にて結合すべきデータを、送信元データおよび送信時刻データによって識別している。送信元データおよび送信時刻データを付与する機能は、一般のパソコンにも備えられている場合が多い。本システムでは、このような一般的な機能を利用しているので、処理を一層簡略化することができる。

【0024】次に、本発明の他の実施の形態を図5～7のフローチャートを用いて説明する。なお、本実施の形態では、前述の実施の形態とは各部の処理のみが異なるので、図2で使用した符号等はそのまま使用する。また、図5～7では、図2～4と同様の処理には同一の符号を付して、処理の詳細な説明を省略する。

【0025】図5は、データの送信が指示されたときパソコン1が実行する処理を表すフローチャートである。図5に示すように、処理を開始すると、送信するデータを読み込み(S 1)、そのデータを二つに分割した(S 3)後、S 31へ移行する。S 31では、現在時刻から乱数等を用いてシリアルナンバーを発生する。なお、シリアルナンバーとしては、アルファベット等の数字以外の符号を含むものを採用してもよい。続くS 33では、1つ目のデータにそのシリアルナンバーおよび数字の「1」を付与し、S 35では、2つ目のデータに上記シリアルナンバーおよび数字の「2」を付与する。続いて、シリアルナンバー等が付与された分割後の各データを、第1および第2のアドレス(サーバ7 aおよび7 bに対応)に送信して処理を終了する(S 5、S 7)。

【0026】図6はサーバ7 a、7 bが繰り返し実行する処理を表すフローチャートである。データを受信すると(S 11: YES) S 41へ移行し、そのデータにシリアルナンバーが付与されているか否かを判断する。付与されている場合(S 41: YES)はS 13へ移行し、データをサーバ5に対応する所定アドレスへ送信してS 11へ移行する。また、データを受信していない場合(S 11: NO)、およびシリアルナンバーが付与されていない場合(S 41: NO)は、そのままS 11へ移行する。すなわち、シリアルナンバーが付与されていない場合は、図5のS 5、S 7によって送信されたデータではないので、図示しない他のルーチンにより、サーバ7 a、7 bとしての通常の処理を行うのである。

【0027】図7は、サーバ5が繰り返し実行する処理

を表すフローチャートである。この処理では、データを受信すると(S21:YES)S51へ移行し、そのデータにシリアルナンバーが付与されているか否かを判断する。付与されている場合(S51:YES)S53へ移行し、既に受信してメモリに格納されているデータの中で、そのデータに付与されたものと同一のシリアルナンバーを有するものがあるか否かを判断する。

【0028】S53で肯定判断した場合、S21にて受信したデータと、既に受信してメモリに格納されていた該当データとは、図5のS5、S7で連続して送信されたデータである。そこで、この場合、二つのデータを結合し(S27)、プリントサーバ11へ送付する(S29)。すると、結合後のデータに基づき、プリンタ13による画像形成が実行される。一方、S21、S51、S53のいずれかで否定判断した場合は、何もせずそのままS21へ戻る。

【0029】本実施の形態でも、前述の実施の形態と同様、データを分割し、異なる通信経路を伝搬させることにより、データの漏洩を良好に防止することができる。また、本システムでは、分割後のデータをシリアルナンバーを用いて対応付けている。このため、データを一層正確に復元することができる。例えば、分割後の各データが長く各データの送信時刻が大幅にずれたとき、すなわち、図5のS5、S7の間隔が大きくなったときなどにも、各データが良好に対応付けられる。更に、データにシリアルナンバーがない場合(S41:NO)、サーバ7a、7bは通常の処理を行う。このため、上記処理のためにサーバ7a、7bを増設する必要もない。

【0030】なお、上記各実施の形態において、S5、S7における送信元データおよび送信時刻データを付与する処理、並びに、S33、S35の処理が識別データ付与手段に、S3の処理がデータ分割手段に、S5、S7におけるデータの送信処理がデータ送信手段に、S21の処理がデータ受信手段に、S27の処理がデータ結合手段に、S23、S25、S51、S53における送信元データ、送信時刻データ、またはシリアルナンバーを抽出する処理が識別データ抽出手段に、それぞれ相当

する。

【0031】また、本発明は、上記実施の形態になんら限定されるものではなく、本発明の要旨を逸脱しない範囲で種々の形態で実施することができる。例えば、本発明は、インターネットを利用したデータ通信システムの他、電話回線やケーブル、無線等、種々の通信経路を利用したデータ通信システムに適用することができる。但し、インターネットはきわめてアクセスが容易である。従って、上記実施の形態のように、インターネットを利用したデータ通信システムに適用した場合、本発明によるデータの漏洩防止の効果が一層顕著になる。

【0032】更に、上記実施の形態では、受信側のサーバ5にプリンタ13を接続したネットワークプリントシステムに対して本発明を適用しているが、本発明は、この他種々のデータ通信システムに適用することができる。例えば、単にデータを送受信するだけのシステムにも適用することができる。この場合、サーバ5のS29の処理(図4、図7)を省略すればよい。

【図面の簡単な説明】

【図1】本発明を適用したデータ通信システムを表す概略構成図である。

【図2】そのシステムの送信側パソコンの処理を表すフローチャートである。

【図3】そのシステムの中継用サーバの処理を表すフローチャートである。

【図4】そのシステムの受信側サーバの処理を表すフローチャートである。

【図5】上記送信側パソコンの処理の他の形態を表すフローチャートである。

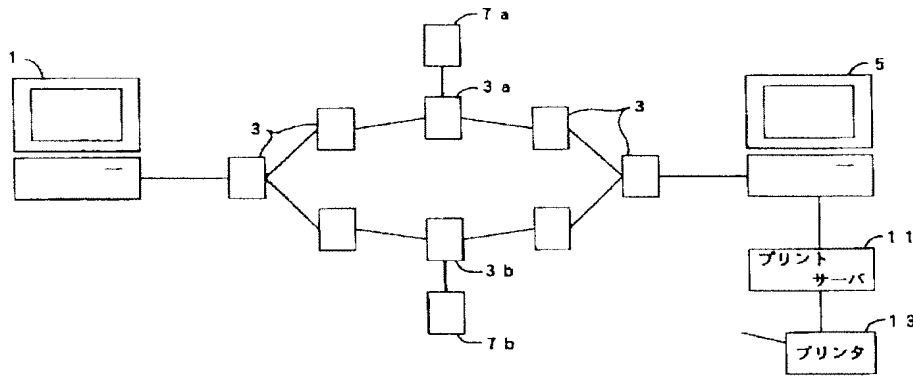
【図6】上記中継用サーバの処理の他の形態を表すフローチャートである。

【図7】上記受信側サーバの処理の他の形態を表すフローチャートである。

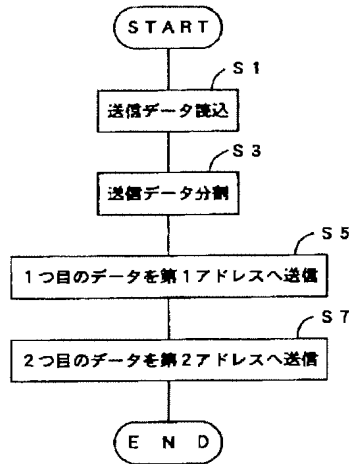
【符号の説明】

- 1…パソコン
- 3…プロバイダ
- 5、7a、7b…サーバ
- 11…プリントサーバ
- 13…プリンタ

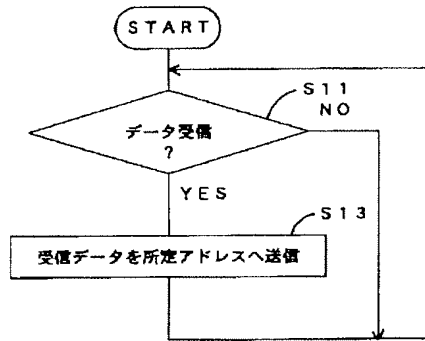
【図1】



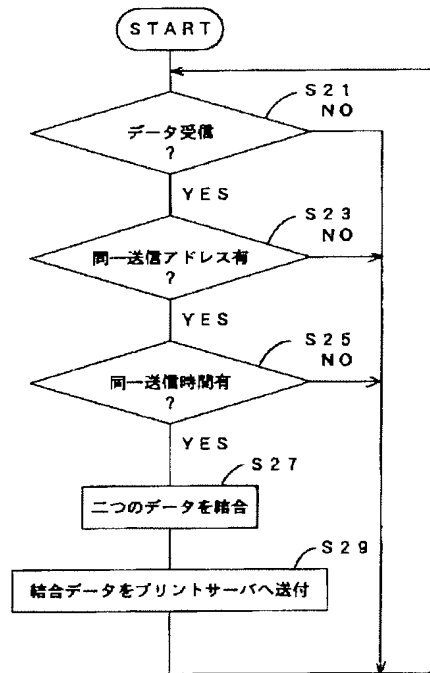
【図2】



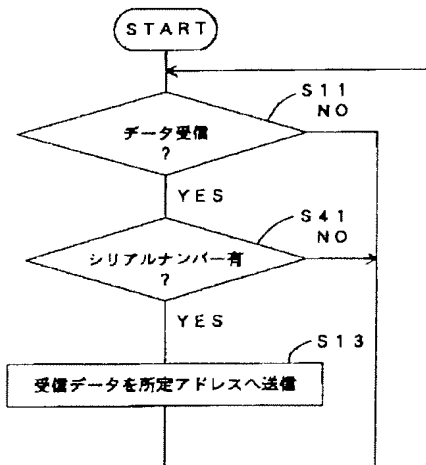
【図3】



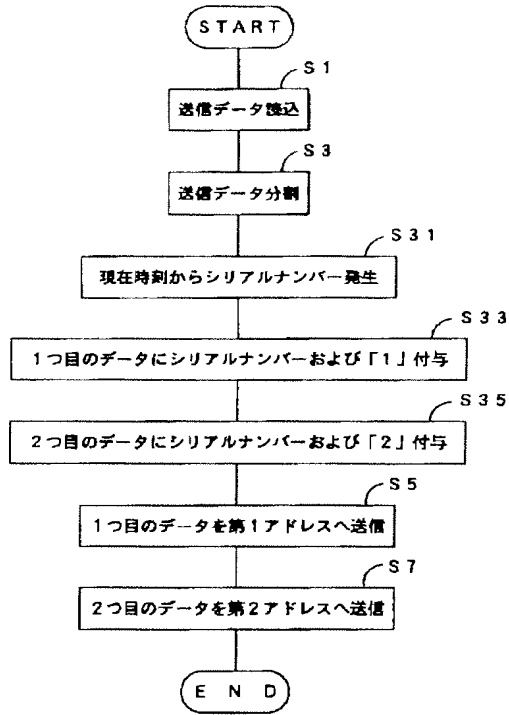
【図4】



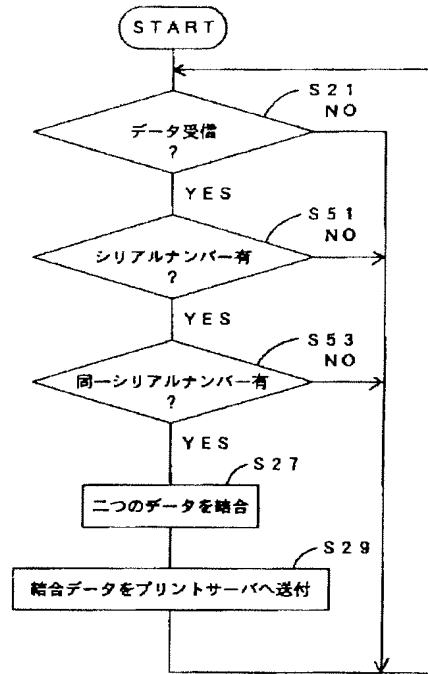
【図6】



【図5】



【図7】



フロントページの続き

(72)発明者 近藤 博大
 愛知県名古屋市瑞穂区苗代町15番1号 プ
 ラザー工業株式会社内

(72)発明者 安井 恒夫
 愛知県名古屋市瑞穂区苗代町15番1号 プ
 ラザー工業株式会社内

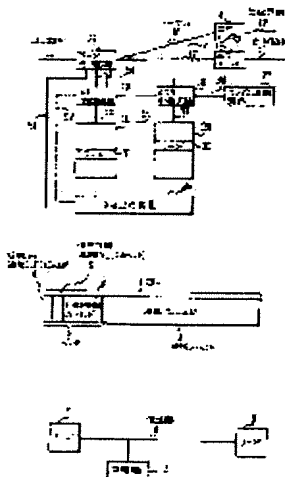
PATENT ABSTRACTS OF JAPAN

(11)Publication number : **04-363941**
(43)Date of publication of application : **16.12.1992**

(51)Int.Cl. **H04L 12/48**
H04L 9/00
H04L 9/10
H04L 9/12

(21)Application number : **03-044062** (71)Applicant : **NIPPON TELEGR & TELEPH
CORP <NTT>**
(22)Date of filing : **18.02.1991** (72)Inventor : **NAKAJIMA SEIICHI
HARADA YONOSUKE**

(54) INTERCEPT PREVENTION METHOD IN ASYNCHRONOUS TRANSFER MODE COMMUNICATION



(57)Abstract:

PURPOSE: To prevent intercept without losing high speed performance of the asynchronous transfer mode(ATM) by using optional one of plural virtual bus identifiers (VPI) and virtual line identifiers (VCI) allocated to one call channel at random so as to transfer a cell.

CONSTITUTION: Plural VPI, VCI are assigned to one call channel and one of the plural VCI, VPI allocated is used at random optionally to transfer a cell. Since the VPI, VCI relating to the same call channel are always changed in the unit of cells through a transmission line 9 between a transmission node and a reception node, even when a cell having the specific VPI, VCI is extracted, it is impossible to collect the communication content of the specific

call. Even when all cells on the transmission line 9 are collected, it is difficult to extract a cell of the specific call and the intercept is prevented. Furthermore, since only the VPI and VCI are revised in the unit of cells, the processing of the header 2 is easy and intercept is prevented without losing the high speed performance of the ATM.

Cited Document 3 (JP-A (Kokai) H04-363941)

<1>

[0019]

[Effects of the Invention]

As explained above, in the method of preventing intercept in ATM communication of the present invention, a plurality of VPIs and VCIs which identify a channel multiplexed by cells are allocated, and are differentiated in each cell. Thus, it is impossible to collect a communication content of a specific call, even when specific VPIs and VCIs are extracted. Accordingly, the method enables prevention of intercept. Furthermore, since only VPIs and VCIs are converted in this method, header processing does not become complicated and a circuit configuration becomes simple. Accordingly, the present method enables prevention of intercept without losing high speed performance of ATM.

<2>

[Explanations of Letters or Numerals]

1, cell; 2, header; 3, information field; 4, virtual path identifier (VPI) field; 5, virtual channel identifier (VCI) field; 6, information field; 7 and 8, nodes; 9, transmission line; 10, eavesdropping device; 11, input transmission line; 12 and 13, output transmission lines; 14 and 15, output buffers; 16 and 17, highways; 21, header processing circuit; 22 and 23, memory control circuits; 24 and 25, memories; 26, central processing device; 27, random selection circuit; 31 and 32, words; 41, 42, 43, 44, and 45, fields; 51, 52, 53, 54, 55, 56, 57, and 58, control lines.

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平4-363941

(43) 公開日 平成4年(1992)12月16日

(51) Int.Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 12/48				
9/00				
9/10				
		8529-5K	H 0 4 L 11/20	Z
		7117-5K	9/00	Z

審査請求 未請求 請求項の数1(全5頁) 最終頁に続く

(21) 出願番号 特願平3-44062

(22) 出願日 平成3年(1991)2月18日

(71) 出願人 000004226

日本電信電話株式会社
東京都千代田区内幸町一丁目1番6号

(72) 発明者 中島 誠一

東京都千代田区内幸町一丁目1番6号 日
本電信電話株式会社内

(72) 発明者 原田 要之助

東京都千代田区内幸町一丁目1番6号 日
本電信電話株式会社内

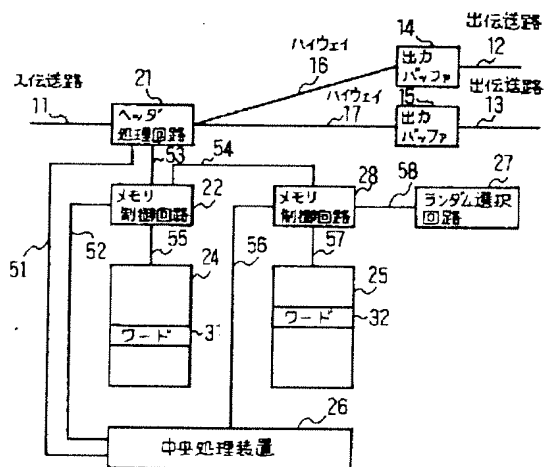
(74) 代理人 弁理士 並木 昭夫

(54) 【発明の名称】 非同期転送モード通信における盗聴防止方法

(57) 【要約】

【目的】 ATM (非同期転送モード) 通信の高速性を損なわずに盗聴防止を可能にする。

【構成】 1つの呼のチャネル (セル多重化されたチャネル) に対して該チャネルを識別する複数のVPI、VCIを割り当て、割り当てられた複数のVPI、VCIの中から任意の一つをランダム選択回路27によりランダムに選択、使用してセルを転送するようにする。



1

【特許請求の範囲】

【請求項1】 非同期転送モード通信において、1つの呼のチャンネルに対して複数の仮想バス識別の割り当て、或いは複数の仮想回線識別の割り当て、の少なくとも一方を実施し、該呼の情報を転送するに際し、セル単位に割り当てられた複数の仮想バス識別の中の任意の一つのランダム使用、或いはセル単位に割り当てられた複数の仮想回線識別の中の任意の一つのランダム使用、の少なくとも一方を実施してセルを転送することを特徴とする非同期転送モード通信における盗聴防止方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、非同期転送モード通信において、セル多重化された回線での情報の盗聴防止方法に関するものである。

【0002】

【従来の技術】高度情報化社会において情報の盗聴防止が重要であることは述べるまでもない。本発明は、かかる意味での非同期転送モード通信における盗聴防止方法に関するものであるが、先ず非同期転送モード通信についての簡単な説明から始める。さて、時分割多重方式には、時間軸上の位置の識別によって多重する方式とラベルの識別によって多重する方式とがある。従来、ラベル多重方式として情報フィールドの長さを可変として多重するパケット方式があるが、最近、固定長のパケット(セル)を用いて多重する方式(被同期転送モード Asynchronous Transfer Mode 以降ATMと略記する)が提案されている。ATMでは、情報転送の要求時のみセルが送出されるので、その頻度に応じて間欠的/連続的通信が可能になり、低速から高速までの任意の転送速度に対応することができ、かつ、情報がない場合には空きセルが挿入されるため、決まったタイミングでセルが出現し、セルの先頭の識別と交換とを高速に行うことができる特徴があり、今後の広帯域ISDNの転送モードとして有望な方式である。なお、ATMについて記載した文献としては、川原崎他、「ATM通信技術の動向—高速広帯域系への展開に向けて—」、電子情報通信学会誌、71,8, pp.809-814(昭63-08)を挙げることができる。

【0003】図3は国際標準のATMセル構造を示す説明図である。同図において、1はセル、2はヘッダ、3は情報フィールド、4は仮想バス識別(VPI)フィールド、5は仮想回線識別(VCI)フィールド、6はその他の制御情報フィールドであり、セル1は53バイト、ヘッダ2は5バイト、情報フィールド3は48バイト、VPIフィールド4は網内では12ビット、ユーザ・網間では8ビット、VCIフィールド5は16ビットで構成される。ヘッダ2には多重、セル交換、トラヒック制御等に必要の制御情報が含まれている。

【0004】ノードにおいて、通常、ハードウェアによ

2

りヘッダ2が分析されて多重、セル交換、トラヒック制御が高速に行われる。多重化された伝送路上の1つの特定のチャンネルは(VPI+VCI)で識別され、交換ノードでVPI, VCIは新たな値に付け替えられる。図4はノード間における盗聴の例を示すブロック図で、7, 8はノード、9は伝送路、10は盗聴機であり、伝送路9にはセル1が転送される。特定のチャンネルを盗聴するには、盗聴機10で特定のVPI, VCIのセルを選択すればよく、容易に盗聴される恐れがある。盗聴を防止する方法には、従来の技術としてはセル1に暗号をかける方式が考えられる。

【0005】しかし、ATMでは伝送速度として数Gbit/s以上の速度までを想定しているため、交換ノードでセルを復号化し、ヘッダ2を分析することは実現不可能である。また、VPI, VCIのみを暗号化しても、暗号化されたVPI, VCIは、交換機における交換時の行先を示す情報であり、常に通信中同じ値をとるので、その値でセルを抽出すれば容易に盗聴されることになる。

【0006】

【発明が解決しようとする課題】本発明は、上記事情に鑑みてなされたもので、その目的とするところはATMの高速性を損なわずに盗聴を防止することのできる非同期転送モード通信における盗聴防止方法を提供することにある。

【0007】

【課題を解決するための手段】本発明は、上記の課題を解決するため、1つの呼のチャンネルに対して複数のVPI, VCIを割り当て、割り当てられたVPI, VCIの中から任意の一つをランダムに使用してセルを転送するようにしたものである。

【0008】

【作用】本発明は、1つの呼のチャンネルに対して複数のVPI, VCIを割り当て、割り当てられた複数のVPI, VCIの中から任意の一つをランダムに使用してセルを転送することを最も特徴とするものである。したがって、送信ノードと受信ノードと間の伝送路において、同一の呼のチャンネルに関するVPI, VCIはセル単位で常に変化するため、特定のVPI, VCIのセルを抽出しても特定の呼の通信内容を収集することは不可能になる。また、伝送路上のすべてのセルを収集したとしても、特定の呼のセルを抽出することは困難であり、盗聴の防止が可能になる。本発明では、VPI, VCIのみをセル単位で変更するため、送信ノード、受信ノードのヘッダ2の処理は容易であり、ATMの高速性を損なうことなく盗聴の防止が可能となる。

【0009】

【実施例】本発明の実施例を図面に基づいて詳細に説明する。説明を簡単にするため、VCIにのみ本発明を適用した場合を例にとって説明する。図1は本発明の盗聴

防止方法を実現する交換ノードの実施例であって、11は入り伝送路、12、13は出伝送路、14、15は出力バッファ、16、17は交換ノード内のハイウェイ、21はヘッダ処理回路、22、23はメモリ制御回路、24、25はメモリ、26は中央処理装置、27はランダム選択回路、31、32はメモリ24、25のワード、41、42、43、44、45はワード32のフィールド、51、52、53、54、55、56、57、58は制御線である。

【0010】メモリ24は、入り伝送路11から到着するセルの「入りVCI」と「変換VCI」との対応をとるメモリであり、入りVCIをアドレスとして変換VCIを得ることができる。メモリ25は「変換VCI」と、「出VCI」との対応をとるメモリであり、変換VCIをアドレスとして出VCIを得ることができる。入り伝送路11からセルが到着すると、ヘッダ処理回路21は入りVCIを制御線53を介してメモリ制御回路22に入力する。

【0011】メモリ制御回路22は、制御線55を介して入りVCIをアドレスとして入力し、メモリ24のワード31から変換VCIを読み出し、変換VCIを制御線54を介してメモリ制御回路23に入力する。メモリ制御回路23は、制御線57を介して変換VCIをアドレスとしてメモリ25に入力し、出VCI(複数)をワード32から読み出し、制御線58を介してランダム選択回路27により、複数の出VCIの中から1つの出VCIを決定し、制御線54、メモリ制御回路22、制御線53を介してヘッダ処理回路21に出VCIを返送し、ヘッダ処理回路21は、該セルの入りVCIをその出VCIに置き換えて、例えばハイウェイ17を介して出力バッファ15に入力する。該セルは出力バッファ15から出伝送路13に送出される。

【0012】1つの呼に関するセルのVCIは複数割り当てられるが、この割り当ては呼の設定時に送信側の交換ノードから呼設定制御セルを用いて、例えば、入りVCIとして#3、#38、#74を使用することを通知してくる。ヘッダ処理回路21がヘッダを分析して呼設定制御セルを検出すると制御線51を介して中央処理装置26に該セルを転送する。中央処理装置26は、出方路の選択制御等に加えて、変換VCI、出VCIを決定する。まず、空きの変換VCIを決定すると、変換VCIをメモリ24の入りVCIに対応するアドレスに書くため、送信側交換ノードから指定された複数のVCIと中央処理装置26が決定した変換VCIを制御線52を介してメモリ制御回路22に転送する。

【0013】メモリ制御回路22は、その指示に従って変換VCIを指定のアドレスに書き込む。例えば、変換VCIを#21とすれば、上記の例ではメモリ24のアドレス#3、#38、#74に変換VCIの#21が書かれる。したがって、該呼のセルの入りVCIが#3、

#38、#74の何れかであれば、変換VCIは#21に変換されることになる。中央処理装置26は同時に、空いた複数の出VCI(例えば#55、#89、#93)を決定し、制御線56を介してメモリ25の変換VCIに対応するアドレスに、複数の出VCIを書き込むため、変換VCIと出VCIをメモリ制御回路23に転送する。

【0014】メモリ制御回路23は、変換VCIに対応するアドレスに出VCI(この例では#55、#89、#93)を書き込む。具体的には、図2に示すワード32のフィールド41~45に、1つのフィールドに1つの出VCIを、例えば#55とか、#89のように、書き込む。この例では3つの出VCIを使用しているため、フィールド41、42、43に#55、#89、#93が各々書き込まれる。メモリ制御回路23は、ワード32を読み出すと、制御線58を介してランダム選択回路27に複数の出VCIを入力し、ランダム選択回路27は乱数を発生して複数の出VCIから1つの出VCIを選択し、制御線58、メモリ制御回路23、制御線54、メモリ制御回路22、制御線53を介してヘッダ処理回路21に該出VCIを返送する。

【0015】このため、ワード32を読み出す毎に、上記の例では出VCIは#55、#89、#93の中の一つがランダムに選択されることになる。従って、入り伝送路11から該呼のセルが到着すると、入りVCIは(#3、#38、#74のいずれかでセル単位に変わる)変換VCIの#21に一旦変換され、出VCIは#55、#89、#93のいずれかに変換されることになる。このため、入り伝送路11、出伝送路13に流れる該呼チャンネルのVCIは固定されず常に変化しており、盗聴を防止することができる。

【0016】上記説明では、割り当て入りVCI、出VCIの数は数個であったが、VCIは16ビットの容量があるため、割り付けるVCIの数を数百以上にすることも特に大きな制約にはならない。上記例では、入りVCI、出VCIの割り当ては呼設定時に行われるため、通信中は割り当てられた複数のVCIは固定されるが、通信中にこれを変更することも可能である。これは、通信中に送信ノードで新たなVCIを決定し、受信ノードでは中央処理装置26からメモリ24、25の内容を書き換えれば良く、この場合にはVCIのランダム性が増加するため、盗聴に対する耐性を高めることが可能となる。

【0017】上記説明では、VCIの複数割り当てを呼設定時に行った例であるが、あらかじめ、ノード間でVCIの割り当てグループを定めておき、その呼設定時にはそのグループ内の1つのVCIを相手ノードに通知する方法をとってもよい。上記説明では、VCIをセル単位で変更する例であったが、さらにVPIをもセル単位に変更する場合、あるいはVPIのみを変更する場合に

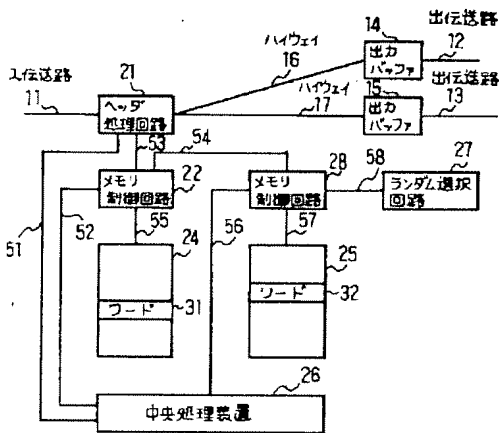
も図1と同様な構成で実現できることは明らかである。

【0018】上記実施例に加えて、入り伝送路1、出伝送路13等には流れる情報に従来行われているスクランブラを掛ければ、さらに盗聴に対する耐力を高めることが可能となる。また、送信ノードから割り当てたVPI、VCIを通知する情報に対して暗号をかければ、さらに盗聴にたいする耐力を高めることが可能となる。上記説明では、特殊な呼が非常に少ない場合には複数のVCIを用いても盗聴の可能性が高いが、ダミーのチャンネルを設定したり、空きセルに複数のVCIを割り当てる等により対処すればよい。

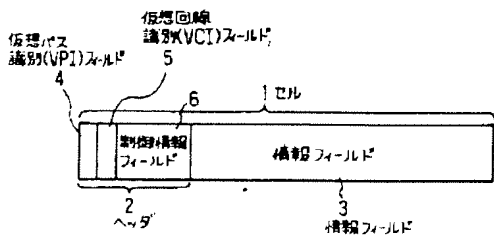
<1>

【0019】
【発明の効果】以上説明したように、本発明のATM通信における盗聴防止方法によれば、セル多重化されたチャンネルを識別するVPI、VCIを複数割り当て、VPI、VCIをセル単位に変更するため、伝送路上で特定VPI、VCIを抽出しても特定呼の通信情報を得ることが不可能であり、盗聴の防止をすることが可能となる。また、本方法ではVPI、VCIのみを変更するため、ヘッダの処理が複雑にならず簡単な回路構成とすることができ、ATMの高速性を損なうことなく盗聴防止

【図1】



【図3】



が実現できる。

【図面の簡単な説明】

【図1】本発明の一実施例を示すブロック図である。

【図2】図1におけるワード32の構成例を示す説明図である。

【図3】ATMセル構造を示す説明図である。

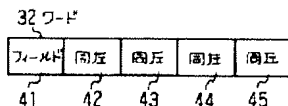
【図4】ノード間における盗聴の例を示すブロック図である。

<2>

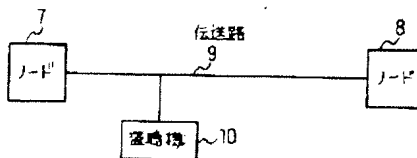
【符号の説明】

1…セル、2…ヘッダ、3…情報フィールド、4…仮想バス識別(VPI)フィールド、5…仮想回線識別(VCI)フィールド、6…情報フィールド、7、8…ノード、9…伝送路、10…盗聴機、11…入り伝送路、12、13…出伝送路、14、15…出力バッファ、16、17…ハイウェイ、21…ヘッダ処理回路、22、23…メモリ制御回路、24、25…メモリ、26…中央処理装置、27…ランダム選択回路、31、32…ワード、41、42、43、44、45…フィールド、51、52、53、54、55、56、57、58…制御線

【図2】



【図4】



【手続補正書】

【提出日】平成4年6月18日

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正内容】

【特許請求の範囲】

【請求項1】 非同期転送モード通信において、1つの

呼のチャンネルに対して複数の仮想バス識別の割り当て、
 或いは複数の仮想回線識別の割り当て、の少なくとも一
 方を実施し、該呼の情報を転送するに際し、セル単位に
 割り当てられた複数の仮想バス識別の中の任意の一つの
 ランダム使用、或いはセル単位に割り当てられた複数の
 仮想回線識別の中の任意の一つのランダム使用、の少な
 くとも一方を実施してセルを転送することを特徴とする
 非同期転送モード通信における盗聴防止方法。

フロントページの続き

(51) Int. Cl.³

識別記号

庁内整理番号

F I

技術表示箇所

H 0 4 L 9/12

PATENT ABSTRACTS OF JAPAN

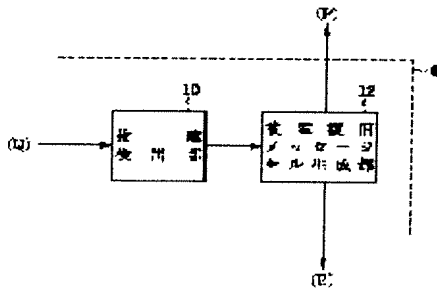
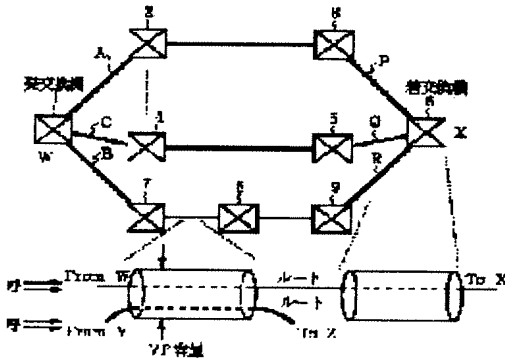
(11)Publication number : 09-018492

(43)Date of publication of application : 17.01.1997

(51)Int.Cl. H04L 12/28
H04L 12/02
H04Q 3/00

(21)Application number : 07-166048 (71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(22)Date of filing : 30.06.1995 (72)Inventor : OKI EIJI
YAMANAKA NAOAKI

(54) ATM COMMUNICATION NETWORK AND FAILURE RESTORATION METHOD



(57)Abstract:

PURPOSE: To reduce the cost of an exchange and further to enforce a fault restoration without providing a device concentratedly restoring a fault by omitting a redundant hardware constitution for securing the high reliability of an exchange.

CONSTITUTION: An incoming exchange 6 is provided with a fault restoration message generation part 12 as a means transmitting a fault restoration message to a virtual pass. A fault restoration message cell has a destination area and a message area. On the destination area, information for reaching a transmitting exchange 1 is mounted via one or more

repeating exchanges 2 to 5 and 7 to 9. The repeating exchanges 2 to 5 and 7 to 9 are

provided with a fault restoration message cell information mounting parts 14 mounting null band information on the repeating exchanges 2 to 5 and 7 to 9 in the message area of the routing fault restoration message cell. By this constitution, constitution, the cost of the exchange is reduced and further, the restoration is made possible without providing a device concentrately performing a fault restoration.

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] An ATM communication network comprising:

Two or more subscriber exchange.

Two or more physical transmission lines which connect between [this] two or more subscriber exchange.

In an ATM communication network which is provided with a transit exchange inserted in two or more of these physical transmission lines and with which a virtual path is set up among said two or more subscriber exchange, to said subscriber exchange. Have a means to send out a fault restoration message cell to a virtual path, and this fault restoration message cell, A means to have a destination area and a message area, and for information for arriving at the destination area via one or more transit exchanges at subscriber exchange of the other party to be carried, and to make empty band region information on the transit exchange carry in a message area of said fault restoration message cell via which it goes in said transit exchange.

[Claim 2] The ATM communication network according to claim 1 provided with a means to add the number of transit exchanges carried in this hop counter field whenever a hop counter field which carries the number of transit exchanges via which it goes in said message area was provided and a fault restoration message cell passed to said transit exchange.

[Claim 3] The ATM communication network according to claim 1 or 2 with which a means to equip said subscriber exchange with a means to recognize the possibility of failure of a transit exchange inserted in a virtual path, and to send out said fault restoration message cell sends out a fault restoration message cell according to an output of this means to recognize.

[Claim 4] Said subscriber exchange is equipped with a means to receive a fault restoration message cell which comes via two or more virtual paths, The ATM communication network according to any one of claims 1 to 3 provided with a means to choose a virtual path used according to the number of empty band region information included in this fault restoration message cell, and transit exchanges.

[Claim 5] a virtual path set as subscriber exchange -- present -- a virtual path of business and

a spare virtual path, and two or more virtual paths that can become being set up beforehand, and, this -- present, when the possibility of failure to a transit exchange inserted in a virtual path of business has been recognized, Said subscriber exchange sends out a fault restoration message cell to a virtual path of said reserve, and two or more virtual paths which can become, respectively, A fault restoration method choosing two or more either virtual path of said reserve or virtual paths which can become according to the number of empty band region information and transit exchanges which were carried in this fault restoration message cell in subscriber exchange used as an address of this fault restoration message cell.

[Claim 6]A way a large number distribute, said subscriber exchange exists in one communications network, and each subscriber exchange performs a fault restoration method according to claim 5 on an autonomous distribution target.

[Claim 7]a virtual path set as subscriber exchange -- present -- a virtual path of business and a spare virtual path, and two or more virtual paths that can become being set up beforehand, and, this -- present, even if there is no failure of a transit exchange inserted in a virtual path of business, Said subscriber exchange sends out a fault restoration message cell to a virtual path of said reserve, and two or more virtual paths which can become, respectively, In subscriber exchange used as an address of this fault restoration message cell. A standby method of fault restoration choosing beforehand two or more either virtual path of said reserve or virtual paths which can become as a spare virtual path candidate according to the number of empty band region information and transit exchanges which were carried in this fault restoration message cell.

[Claim 8]A way a large number distribute, said subscriber exchange exists in one communications network, and each subscriber exchange performs a standby method of the fault restoration according to claim 7 on an autonomous distribution target.

[Claim 9]A fault restoration method, wherein it addresses subscriber exchange in one communications network to other subscriber exchange belonging to self which sets a virtual path as self, and/or its communications network and it sends out a fault restoration message cell to a virtual path, respectively.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Industrial Application]This invention is used for an ATM (Asynchronous Transfer Mode) communications network. It is related with the fault restoration art over failure of the communication apparatus especially inserted in the transmission line.

[0002]

[Description of the Prior Art]The virtual channel hair drier (Virtual Channel Handler,

switchboard) which switches by an ATM communication network making a unit physically a virtual channel (Virtual Channel: it is called following VC), It is connected by the transmission line and the virtual path handler (Virtual Path Handler: VPH or cross connect, XC) which sets up the route of information transfer by making a virtual path (Virtual Path: henceforth VP) into a unit is constituted. Theoretically, between VCH is connected by VP and the termination of VP is carried out by VCH via zero or one or more VPH(s).

[0003]The fault restoration method for failure of the conventional communication apparatus is shown in drawing 12. Drawing 12 is a figure showing the concept of the conventional fault restoration method. There is fault restoration of VP level shown in the fault restoration and drawing 12 (a) of the physical level shown in drawing 12 (b) in the conventional fault restoration method. making the physical transmission-line link double, in order to realize fault restoration of a physical level -- one side -- present -- business -- a system and another side are made into the reserve system. if -- present -- business -- if failure occurs in the communication apparatus of a system -- present -- business -- it changes from a system to a reserve system, and failure is restored. However, in the fault restoration of a physical level, a physical transmission-line link must be made double and there is always a problem that a network resource cannot be used efficiently.

[0004]Then, there is the fault restoration method of VP level which applied the concept of VP which is the feature of an ATM communication network. VP is identified by VPI (Virtual Path Identifier) in the header area given to the cell which is a functional information unit, and a course is set up in VPH by the pass connection (routing) table which described the connection destination of the path. Fault restoration of VP level is realized by switching VP cut by failure to VP which bypassed the locating fault and was newly formed using the ability of the course and capacity of VP to set up independently. It is based on the detour path information to which the central post office which is supervising the ATM communication network unitary was especially set beforehand at the time of a failure occurrence, and is each node () within the net. [VCH and] The fault restoration method with which a centralized control system and each node make an autonomous distribution target look for and restore a detour path for the method which controls to VPH and others is called self healing method. As compared with the fault restoration of a physical level, it excels in the fault restoration of VP level with the point that the network resource of a transmission line can be used efficiently, or the point that it can respond to change of a net flexibly. Therefore, the fault restoration method which combined the physical level and VP level is applied as the conventional fault restoration method.

[0005]

[Problem(s) to be Solved by the Invention]However, in the fault restoration method of only the conventional physical level and VP level, sake [premised], a high reliability switchboard is required for failure of VCH (switchboard). In the ATM communication

network with which two or more media are intermingled, although the reliability demanded for every media differed, the switchboard was designed satisfy reliability according to the reliability demanded most highly, and it was redundant not much to the media which do not require reliability. Although drawing 13 is a key map of the high-reliability-ized switchboard, in the high-reliability-ized switchboard, the switch part, the I/O part, and the CPU section have doubled like drawing 13, and these units are further combined by the crossing route. The cost of the high-reliability-ized switchboard will become high about 6 times from 4 times compared with the cost of a switchboard with simple composition by such double-ization.

[0006]This invention is carried out to such a background and is a thing.

It is providing the ATM communication network and the fault restoration method of performing the measure against fault restoration on condition of the purpose.

An object of this invention is to provide the ATM communication network and the fault restoration method the redundant hardware constitutions for securing the high-reliability of a switchboard are omissible. An object of this invention is to provide the ATM communication network and the fault restoration method of reducing the cost of a switchboard. An object of this invention is to provide the ATM communication network and the fault restoration method of performing fault restoration, without forming the device which performs fault restoration intensively.

[0007]

[Means for Solving the Problem]When applying a switchboard with simple composition as a communication apparatus, it is necessary to restore quickly VC route obstacle at the time of failure of a switchboard. Then, this invention provides a method of restoring VC route obstacle quickly at the time of failure of a switchboard. As the method, at the time of failure of a switchboard, in order to restore a working route obstacle between arrival-and-departure switchboards, a fault restoration message cell is sent out from an incoming exchange, A switchboard exchanges information with an autonomous distribution target, and notifies reticulated voice to *****, a route is changed, and a route obstacle by switchboard failure is restored by VC route level. This is called self healing of VC route level.

[0008]In conventional technology, although self healing of VP level was performed, there is a place by which it is characterized [of this invention] in the ability to restore VC route obstacle at the time of switchboard failure by self healing of VC route level.

[0009]That is, the first viewpoint of this invention is an ATM communication network which is provided with two or more physical transmission lines which connect between [this] two or more subscriber exchange with two or more subscriber exchange, and a transit exchange inserted in two or more of these physical transmission lines and with which a virtual path is set up among said two or more subscriber exchange.

[0010]Here a place by which it is characterized [of this invention] to said subscriber

exchange. Have a means to send out a fault restoration message cell to a virtual path, and this fault restoration message cell, Have a destination area and a message area, it is carried by information for arriving at the destination area via one or more transit exchanges at subscriber exchange of the other party, and to said transit exchange. It is in a place provided with a means to make empty band region information on the transit exchange carry in a message area of said fault restoration message cell via which it goes.

[0011]Whenever a hop counter field which carries the number of transit exchanges via which it goes in said message area is provided and a fault restoration message cell passes to said transit exchange, it is desirable to have a means to add the number of transit exchanges carried in this hop counter field.

[0012]As for a means to equip said subscriber exchange with a means to recognize the possibility of failure of a transit exchange inserted in a virtual path, and to send out said fault restoration message cell, it is desirable to send out a fault restoration message cell according to an output of this means to recognize.

[0013]It is desirable to equip said subscriber exchange with a means to receive a fault restoration message cell which comes via two or more virtual paths, and to have a means to choose a virtual path used according to the number of empty band region information included in this fault restoration message cell and transit exchanges.

[0014]A place by which the second viewpoint of this invention is the fault restoration method, and it is characterized [the], a virtual path set as subscriber exchange -- present -- a virtual path of business and a spare virtual path, and two or more virtual paths that can become being set up beforehand, and, this -- present, when the possibility of failure to a transit exchange inserted in a virtual path of business has been recognized, Said subscriber exchange sends out a fault restoration message cell to a virtual path of said reserve, and two or more virtual paths which can become, respectively, In subscriber exchange used as an address of this fault restoration message cell, it is in a place which chooses two or more either virtual path of said reserve or virtual paths which can become according to the number of empty band region information and transit exchanges which were carried in this fault restoration message cell.

[0015]It is the feature that a large number distribute, said subscriber exchange exists in one communications network in this fault restoration method, and each subscriber exchange performs this fault restoration method on an autonomous distribution target.

[0016]A place by which the third viewpoint of this invention is a fault restoration standby method, and it is characterized [the], a virtual path set as subscriber exchange -- present -- a virtual path of business and a spare virtual path, and two or more virtual paths that can become being set up beforehand, and, this -- present, even if there is no failure of a transit exchange inserted in a virtual path of business, Said subscriber exchange sends out a fault restoration message cell to a virtual path of said reserve, and two or more virtual paths which

can become, respectively, In subscriber exchange used as an address of this fault restoration message cell. It is in a place which chooses beforehand two or more either virtual path of said reserve or virtual paths which can become as a spare virtual path candidate according to the number of empty band region information and transit exchanges which were carried in this fault restoration message cell.

[0017]It is the feature that a large number distribute, said subscriber exchange exists in one communications network in this fault restoration standby method, and each subscriber exchange performs this fault restoration standby method on an autonomous distribution target.

[0018]A place by which the fourth viewpoint of this invention is the fault restoration method, and it is characterized [the], Subscriber exchange in one communications network is in a place which addresses to other subscriber exchange belonging to self which sets a virtual path as self, and/or its communications network, and sends out a fault restoration message cell to a virtual path, respectively.

[0019]Although that expression [like] which is a communication apparatus which is different in subscriber exchange and a transit exchange is used in this specification, this is for explaining plainly and a communication apparatus of the same hardware constitutions can realize it.

[0020]

[Function]In the method of this invention, by self healing of VC route level. Since a fault restoration message cell is sent out from an incoming exchange, a switchboard can exchange information with an autonomous distribution target, and can notify reticulated voice to ***** , a route can be changed and VC route obstacle at the time of switchboard failure can be restored, The necessity which uses a high reliability switchboard is lost and cost reduction is planned by using a switchboard with simple composition.

[0021]The fault restoration message cell which an incoming exchange sends out reaches ***** via a virtual path. The virtual path beforehand defined as a virtual path which can turn into a spare virtual path may be sufficient as this virtual path, and the unspecified virtual path in which failure is not recognized may be sufficient as it.

[0022]A fault restoration message cell collects the empty band region information on the virtual path passed while reaching ***** from an incoming exchange. If a way of speaking is changed, the transit exchange inserted in the virtual path to pass carries the empty band region information in a self transit exchange in the message area of a fault restoration message cell, when passing a fault restoration message cell. The number of the transit exchanges passed simultaneously also carries as information. In ***** , empty band region information and a number of a transit exchange of passed information are referred to, and the virtual path optimal as a spare virtual path is chosen. Henceforth, a virtual channel is set as this virtual path, and communication is resumed.

[0023]sending out of a fault restoration message cell -- present -- the virtual path of business -- or -- present -- it may control to be carried out when a certain failure has been recognized by the transit exchange on the virtual path of business -- by carrying out. Or it is also good to send out a fault restoration message cell also at the time of usual, and to always choose the virtual path candidate optimal as a spare virtual path.

[0024]In this invention, it is characterized [main] by each switchboard contained in an ATM communication network carrying out such fault restoration control to autonomous distribution.

[0025]

[Example]

(The first example) The composition of the first example of this invention is explained with reference to drawing 1 - drawing 5. Drawing 1 is an entire configuration figure of this invention. Drawing 2 is an important section block lineblock diagram of an incoming exchange. Drawing 3 is a lineblock diagram of a fault restoration message cell. Drawing 4 is an important section block lineblock diagram of a transit exchange. Drawing 5 is an important section block lineblock diagram of *****.

[0026]***** 1 and the incoming exchange 6 whose this invention is subscriber exchange, and physical transmission-line P-R which connects this ***** 1 and between incoming-exchange 6, It is an ATM communication network which is provided with the transit exchanges 2, 3, 4, 5, 7, 8, and 9 inserted in this physical transmission-line P-R and with which a virtual path is set up between ***** 1 and the incoming exchange 6.

[0027]Here the place by which it is characterized [of this invention] to the incoming exchange 6. Have the fault restoration message cell generation part 12 as a means to send out a fault restoration message cell to a virtual path, and this fault restoration message cell, Have the destination area H and message area M, and the information for arriving at the destination area H at ***** 1 via the one or more transit exchanges 2, 3, 4, 5, 7, 8, and 9 is carried, It is in the place which equipped the transit exchanges 2, 3, 4, 5, 7, 8, and 9 with the fault restoration message cell information mount part 14 as a means which makes the empty band region information on the transit exchanges 2, 3, 4, 5, 7, 8, and 9 carry in message area M of the fault restoration message cell via which it goes.

[0028]In this invention example, in order to explain plainly, express as if it was the communication apparatus provided with hardware constitutions which are different, respectively in ***** 1, the incoming exchange 6, and the transit exchanges 2, 3, 4, 5, 7, 8, and 9, but. These are realizable as one communication apparatus provided with each function in common.

[0029]It is provided by hop counter field HC which carries the number of the transit exchanges 2, 3, 4, 5, 7, 8, and 9 via which it goes in message area M, and to the transit exchanges 2, 3, 4, 5, 7, 8, and 9. Whenever a fault restoration message cell passes, a means

to add the number of the transit exchanges carried in this hop counter field HC was combined with the fault restoration message cell information mount part 14, and it has it. [0030]***** 1 and the incoming exchange 6 are equipped with the failure detection part 10 as the transit exchanges 2, 3, 4, 5, 7, and 8 inserted in the virtual path, and a means to recognize the possibility of failure of nine, The fault restoration message cell generation part 12 sends out a fault restoration message cell according to the output of this failure detection part 10.

[0031]***** 1 is equipped with the spare-routes set part 16 as a means which receives the fault restoration message cell which comes via two or more virtual paths, A means to choose the virtual path used according to the number of the empty band region information included in this fault restoration message cell and transit exchanges was combined with the spare-routes set part 16, and it has it.

[0032]VC route is set as the incoming exchange 6 through one or more VP from ***** 1. In ***** 1, when a call occurs, a certain route is chosen from two or more VC routes, and a call admission judging (Connection Admission Control:CAC) is performed. For example, selection of a route is chosen at random. It becomes call loss, if a call is received by CAC, VC connection will be set up and a call will not be received by it.

[0033]Next, operation of the first example of this invention is explained with reference to drawing 6. Drawing 6 is a figure for explaining operation of the first example of this invention. As shown in drawing 6, only paying attention to one working route, the failure recovery method of the first example of this invention when failure occurs is shown in the transit exchange 5. The working route (1->4->5->6) is set up via two transit exchanges between ***** 1 and the incoming exchange 6, a working route is this time, and it is B. The zone of [Mbps] is used.

[0034]To this working route, a call is received after CAC, and VC connection is set up or it is cut. The usage band of this working route is called for, for example in ***** 1 by observing the number of cells currently used by the working route in a certain window size. There are a jumping window and a sliding window as a window used for observation.

[0035]Here, a jumping window is the observation method which changes without a window position (observation post) overlapping with a constant period, and a sliding window is the observation method which changes gradually, while a window position overlaps with a constant period. When it says very roughly, observation with a high-speed jumping window is an advantage, and observation with an exact sliding window is an advantage.

[0036]In drawing 6 which prepares for a working route becoming unusable and sets up two or more spare routes beforehand by failure, two spare routes (the route P:1->2->3->6, the route R:1->7->8->9->6) are set up. When failure occurs, the switchboard 1 from a twist and the incoming exchange 6 recognize that a working route is in an unusable state to the cell which notifies alarm, and others. the call of VC newly demanded after a failure occurrence

although relief of VC connection set as the working route at present is not performed -- the maximum reception ***** -- an alternative route is searched like. Here, the sender and ***** 1 to which the incoming exchange 6 sends out a fault restoration message cell serve as Chooser which receives a fault restoration message cell, changes it out of spare routes, and chooses a route. The incoming exchange (sender) 6 sends out a fault restoration message cell, in order to investigate the state to spare routes. A fault restoration message cell investigates the state of VP on the course of the spare routes P and R in accordance with the course of the spare routes P and R. The route R is raised to an example and explained. Minimum b_{min} (4) channel-information RD of a (1) hop counter HC(2) hop limit HL(3) VP intact zone is written in message area [of a fault restoration message cell] M as a pay load. The hop limit HL is beforehand set up in consideration of delay conditions and others. The value of minimum b_{min} is made into infinity and the value of minimum b_{min} is written in the fault restoration message cell. The fault restoration message cell which goes via the route R is sent out to the transit exchange 9 from the incoming exchange 6, and in the transit exchange 9, if it $b < B_{min}$ Becomes, it will make the value of the intact VP zone b b_{min} . In the transit exchange 9, b is called for, when VP intact zone in a certain window size observes the number of use cells. There are a jumping window and a sliding window as a window used for observation. Hop counter HC is further sent out to the following switchboard, unless it counts up one and the hop limit HL is exceeded, whenever it goes via the transit exchange 9->8->7. However, spare routes are usually set up beforehand not exceed a hop limit. In the following switchboard 8, it is $b = 2$, and since it is $b < B_{min}$, it is set to $b_{min} = 2$. Repeating the process of fault restoration message cell sending out similarly, a fault restoration message cell reaches ***** 1. The fault restoration message cell A sent out on spare-routes P reaches ***** 1 similarly. One or more ***** 1 are chosen as a route of a switch destination from the spare routes P or R in consideration of the usage band B, and the spare-routes information (minimum b_{min} of VP intact zone, hop number) and others of a working route. In the example of drawing 7, although drawing 7 is a figure showing the route change situation in the first example of this invention, since the minimum of VP intact zone is [the route P] the largest in spare routes, the route P is chosen as a route of a switch destination, and the route P is used as a working route after fault restoration.

[0037]Therefore, since a switchboard exchanges information with an autonomous distribution target by sending out of a fault restoration message cell, a route is changed at the time of failure of a switchboard and failure is restored, Even if it is not a high reliability switchboard like before made double, using a switchboard with simple composition, or since it can do, the cost reduction of a switchboard can be planned.

[0038]The (second example), next the second example of this invention are described with reference to drawing 8. Drawing 8 is a figure for explaining operation of the second example of this invention. Although the fault restoration message cell was sent out in the first

example of this invention at the time of a failure occurrence, At the second example of this invention, it is usually the incoming exchange (sender) 6 to RM (Resource Management) also by the time like drawing 8. A cell is sent out and the state of the spare routes P and R is supervised. Operation of an RM cell is the same as operation of the fault restoration message cell of the first example of this invention. Out of the spare routes P or R, in consideration of the usage band B, and the spare-routes information (minimum b_{min} of VP intact zone, hop number) and others of a working route, it has ***** (Chooser) 1 at the time of the obstacle of a working route, and it determines the route of the switch destination.

[0039]Here, an RM cell is periodically sent out from the incoming exchange (sender) 6, and ***** (Chooser) 1 which received the RM cell updates the route of the switch destination according to reticulated voice. The sending-out interval of an RM cell is determined from the degree of change of reticulated voice.

[0040]When failure occurs, the switchboard 1 from a twist recognizes that a working route is in an unusable state to the cell which notifies alarm, and others. The switchboard 1 from ***** is changed to the switch destination route with which it equipped usual at the time of a working route obstacle, and the obstacle of a working route is used as a working route.

[0041]Therefore, shortening of fault restoration time can be attained by sometimes sending out RM (Resource Management) cell from the incoming exchange (sender) 6, sometimes supervising the state of spare routes, and usually deciding the switch destination route to be it in preparation for the time of the obstacle of a working route.

[0042]The (third example), next the third example of this invention are described with reference to drawing 9. Drawing 9 is a figure for explaining operation of the third example of this invention. In the first example of this invention, the spare routes P and R were set up beforehand, and the fault restoration message cell was sent out on spare-routes P and R at the time of a failure occurrence. In the third example of this invention, the spare routes P and R are not set up beforehand, but a fault restoration message cell is sent out with flooding (Flooding) like drawing 9, and ***** 1 chooses spare routes according to the fault restoration message cell which reached ***** 1.

[0043]Here, flooding is "Flood, i.e., the term based on the image of sending out a cell to the unspecified direction just like a "flood",", and it uses for the meaning of sending out a fault restoration message cell to all the switchboards which send out VP to a self-switchboard.

[0044]As the first example of this invention explained, minimum b_{min} (4) channel-information RD of a (1) hop counter HC(2) hop limit HL(3) VP intact zone is written in the pay load of a fault restoration message cell. The hop limit HL is beforehand set up in consideration of delay conditions and others. The value of minimum b_{min} is made into infinity and the value of minimum b_{min} is written in the fault restoration message cell.

[0045]First, the incoming exchange (sender) 6 sends out a fault restoration message cell to all the switchboards which send out VP to a self-switchboard. The switchboard which

received the fault restoration message cell will make the value of the intact VP zone b_{\min} , if it $b < B_{\min}$ Becomes. In a switchboard, b is called for, when VP intact zone in a certain window size observes the number of use cells. The information on the switchboard via which it went is written in as channel information. Whenever hop counter HC goes via a switchboard, one is counted up, and if it is over the hop limit HL or has already gone via the same switchboard by channel information RD, a fault restoration message cell will be discarded. Otherwise, a fault restoration message cell is further sent out to all the switchboards which send out VP to a self-switchboard, the switchboard which received the fault restoration message cell repeats the same operation, and a fault restoration message reaches *****.

[0046]One or more ***** (Chooser) 1 are chosen from the fault restoration message cell which arrived as a route of a switch destination in consideration of the route information (minimum b_{\min} of VP intact zone, hop number) and others based on the usage band B and the fault restoration message cell which arrived of a working route.

[0047]Therefore, fault restoration which was flexibly equivalent to net topology, VP capacity, and other change can be performed by sending out a fault restoration message cell with flooding, and making a fault restoration message cell reach ***** 1, without setting up spare routes beforehand.

[0048]The fault restoration concept by the fault restoration method of this invention is shown in drawing 10 and drawing 11. Drawing 10 is a figure showing the concept of the fault restoration method of this invention. Drawing 11 is a key map of the ATM communication network which applied the fault restoration method of this invention. Drawing 10 (b) and (c) is a fault restoration concept of VP level and a physical level known from the former. An ATM communication network can consist of this inventions, without using a highly reliable switchboard by performing fault restoration of VC route level, as shown in drawing 11 as shown in drawing 10 (a).

[0049]

[Effect of the Invention]As explained above, according to this invention, fault restoration control on condition of failure of a switchboard can be performed. For this reason, the redundant hardware constitutions for securing the high-reliability of a switchboard are omissible. Therefore, the cost of a switchboard can be reduced. Fault restoration can be performed without forming the device which performs fault restoration intensively.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]The entire configuration figure of this invention.

[Drawing 2]The important section block lineblock diagram of an incoming exchange.

[Drawing 3]The lineblock diagram of a fault restoration message cell.

[Drawing 4]The important section block lineblock diagram of a transit exchange.

[Drawing 5]The important section block lineblock diagram of *****.

[Drawing 6]The figure for explaining operation of the first example of this invention.

[Drawing 7]The figure showing the route change situation in the first example of this invention.

[Drawing 8]The figure for explaining operation of the second example of this invention.

[Drawing 9]The figure for explaining operation of the third example of this invention.

[Drawing 10]The figure showing the concept of the fault restoration method of this invention.

[Drawing 11]The key map of the ATM communication network which applied the fault restoration method of this invention.

[Drawing 12]The figure showing the concept of the conventional fault restoration method.

[Drawing 13]The key map of the high-reliability-ized switchboard.

[Description of Notations]

1 *****

2-5, 7-9 Transit exchange

6 Incoming exchange

10 Failure detection part

12 Fault restoration message cell generation part

14 Fault restoration message cell information mount part

16 Spare-routes set part

H Destination area

HC Hop counter

HL Hop limit

M Message area

RD Channel information

b_{\min} minimum

P, Q, and R Route

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-18492

(43) 公開日 平成9年(1997)1月17日

(51) Int.Cl.*	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 12/28		9466-5K	H 0 4 L 11/20	D
			H 0 4 Q 3/00	
H 0 4 Q 3/00		9466-5K	H 0 4 L 11/02	A

審査請求 未請求 請求項の数 9 O L (全 9 頁)

(21) 出願番号 特願平7-166048

(22) 出願日 平成7年(1995)6月30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 大木 英司

東京都千代田区内幸町一丁目1番6号 日
本電信電話株式会社内

(72) 発明者 山中 直明

東京都千代田区内幸町一丁目1番6号 日
本電信電話株式会社内

(74) 代理人 弁理士 井出 直孝 (外1名)

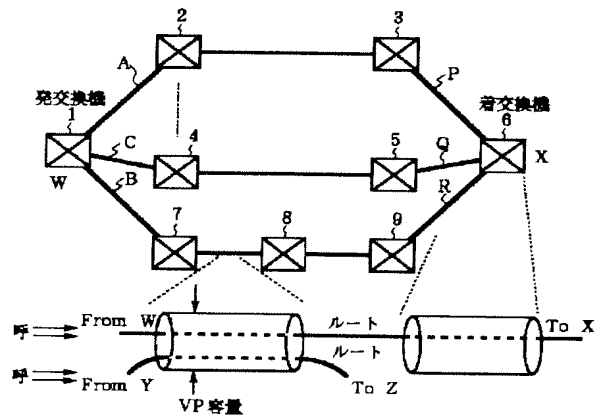
(54) 【発明の名称】 ATM通信網および故障復旧方法

(57) 【要約】

【目的】 交換機の故障を前提とした故障復旧対策を行う。

【構成】 交換機の故障時に、着交換機から故障復旧メッセージを送出して交換機が自律分散的に情報を交換し、発交換機に網状態を通知してルートの切替えを行い、交換機故障によるルート障害がV Cルートレベルにより復旧される。

【効果】 交換機の高信頼性を確保するための冗長なハードウェア構成を省略することができる。このため交換機のコストを低減することができる。さらに、集中的に故障復旧を行う装置を設けることなく故障復旧を行うことができる。



【特許請求の範囲】

【請求項1】 複数の加入者交換機と、この複数の加入者交換機相互間を接続する複数の物理伝送路と、この複数の物理伝送路に介挿される中継交換機とを備え、前記複数の加入者交換機の間にはバーチャルパスが設定されるATM通信網において、

前記加入者交換機には、バーチャルパスに故障復旧メッセージセルを送出する手段を備え、この故障復旧メッセージセルは、宛先領域およびメッセージ領域を有し、その宛先領域に一年以上の中継交換機を経由して相手側の加入者交換機に到達するための情報が搭載され、

前記中継交換機には、経由する前記故障復旧メッセージセルのメッセージ領域にその中継交換機の空帯域情報を搭載させる手段を備えたことを特徴とするATM通信網。

【請求項2】 前記メッセージ領域には、経由する中継交換機の数に搭載するホップカウンタ領域が設けられ、前記中継交換機には、故障復旧メッセージセルが通過する毎にこのホップカウンタ領域に搭載された中継交換機の数に算入する手段を備えた請求項1記載のATM通信網。

【請求項3】 前記加入者交換機には、バーチャルパスに介挿された中継交換機の故障の可能性を認識する手段を備え、前記故障復旧メッセージセルを送出する手段は、この認識する手段の出力にしたがって故障復旧メッセージセルを送出する請求項1または2記載のATM通信網。

【請求項4】 前記加入者交換機には、複数のバーチャルパスを介して到来する故障復旧メッセージセルを受信する手段を備え、この故障復旧メッセージセルに含まれる空帯域情報および中継交換機の数にしたがって利用するバーチャルパスを選択する手段を備えた請求項1ないし3のいずれかに記載のATM通信網。

【請求項5】 加入者交換機に設定されるバーチャルパスには現用のバーチャルパスおよび予備のバーチャルパスとなりうる複数のバーチャルパスがあらかじめ設定され、この現用のバーチャルパスに介挿される中継交換機に故障の可能性が認識されたとき、前記加入者交換機は故障復旧メッセージセルを前記予備のバーチャルパスとなりうる複数のバーチャルパスにそれぞれ送出し、この故障復旧メッセージセルの宛先となる加入者交換機では、この故障復旧メッセージセルに搭載された空帯域情報および中継交換機の数にしたがって前記予備のバーチャルパスとなりうる複数のバーチャルパスのいずれかを選択することを特徴とする故障復旧方法。

【請求項6】 前記加入者交換機は一つの通信網の中に多数分散して存在し、各加入者交換機が請求項5記載の故障復旧方法を自律分散的に実行する方法。

【請求項7】 加入者交換機に設定されるバーチャルパスには現用のバーチャルパスおよび予備のバーチャルパス

となりうる複数のバーチャルパスがあらかじめ設定され、この現用のバーチャルパスに介挿される中継交換機の故障がなくても、前記加入者交換機は故障復旧メッセージセルを前記予備のバーチャルパスとなりうる複数のバーチャルパスにそれぞれ送出し、この故障復旧メッセージセルの宛先となる加入者交換機では、この故障復旧メッセージセルに搭載された空帯域情報および中継交換機の数にしたがって前記予備のバーチャルパスとなりうる複数のバーチャルパスのいずれかを予備のバーチャルパス候補としてあらかじめ選択することを特徴とする故障復旧の待機方法。

【請求項8】 前記加入者交換機は一つの通信網の中に多数分散して存在し、各加入者交換機が請求項7記載の故障復旧の待機方法を自律分散的に実行する方法。

【請求項9】 一つの通信網内にある加入者交換機は自己にバーチャルパスを設定する自己およびまたはその通信網に属する他の加入者交換機に宛てて故障復旧メッセージセルをバーチャルパスにそれぞれ送することを特徴とする故障復旧方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明はATM（非同期転送モード）通信網に利用する。特に、伝送路に介挿された通信装置の故障に対する故障復旧技術に関する。

【0002】

【従来の技術】 ATM通信網は、物理的には、バーチャルチャネル(Virtual Channel: 以下VCという)を単位としてスイッチングを行うバーチャルチャネルハンドラ(Virtual Channel Handler、交換機)と、バーチャルパス(Virtual Path: 以下VPという)を単位として情報転送の方路を設定するバーチャルパスハンドラ(Virtual Path Handler: VPH、またはクロスコネクタ、XC)とが伝送路により接続されて構成される。理論的には、VCH間がVPにより接続され、VPは零または1以上のVPHを経由してVCHで終端される。

【0003】 従来の通信装置の故障に対する故障復旧方法を図12に示す。図12は従来の故障復旧方法の概念を示す図である。従来の故障復旧方法には、図12

(b)に示す物理レベルの故障復旧と図12(a)に示すVPレベルの故障復旧がある。物理レベルの故障復旧を実現するためには、物理伝送路リンクを2重化しておく、一方を現用系、もう一方を予備系としておく。もし、現用系の通信装置に故障が発生したら、現用系から予備系に切替えられ、故障が復旧される。しかし、物理レベルの故障復旧では、常時、物理伝送路リンクを2重化しておかなければならず、網リソースを効率的に利用できないという問題がある。

【0004】 そこで、ATM通信網の特徴であるVPの概念を適用したVPレベルの故障復旧方法がある。VPは、情報転送単位であるセルに付与されたヘッダ領域中

10

20

30

40

50

のVPI (Virtual Path Identifier) により識別され、VPHにおいては、パスの接続先を記述したパス接続(ルーティング)テーブルにより経路が設定される。VPレベルの故障復旧は、VPの経路と容量が独立に設定できることを利用して、故障により切断されたVPを、故障箇所を迂回して新たに形成されたVPに切り換えることにより実現される。特に、故障発生時に、ATM通信網を一元的に監視している集中局があらかじめ設定された迂回パス情報に基づき網内の各ノード(VCH、VPHその他)に対して制御を行う方式を集中制御方式、各ノードが自律分散的に迂回パスを探索・復旧させる故障復旧方式をセルフヒーリング方式という。VPレベルの故障復旧では、物理レベルの故障復旧と比較して、伝送路の網リソースを効率良く利用できる点や網の変化に柔軟に対応できる点で、優れている。したがって、従来の故障復旧方法として、物理レベルとVPレベルとを組み合わせた故障復旧方法が適用されている。

【0005】

【発明が解決しようとする課題】しかし、従来の物理レベルとVPレベルのみの故障復旧方法では、VCH(交換機)の故障は前提とされないため、高信頼な交換機が必要である。また、複数のメディアが混在するATM通信網においては、メディア毎に要求される信頼度が異なるが、最も高く要求される信頼度に合わせて信頼性を満足するように交換機が設計されており、あまり、信頼度を要求しないメディアに対しては、冗長であった。図13は高信頼化された交換機概念図であるが、高信頼化された交換機では、図13のようにスイッチ部、I/O部、およびCPU部が二重化されており、さらに、これらのユニットはクロスルートで結合されている。このような二重化によって高信頼化された交換機のコストは、単純な構成を持つ交換機のコストと比べ、4倍から6倍程度高くなってしまふ。

【0006】本発明は、このような背景に行われたものであり、交換機の故障を前提とした故障復旧対策を行うことができるATM通信網および故障復旧方法を提供することを目的とする。本発明は、交換機の高信頼性を確保するための冗長なハードウェア構成を省略することができるATM通信網および故障復旧方法を提供することを目的とする。本発明は、交換機のコストを低減することができるATM通信網および故障復旧方法を提供することを目的とする。本発明は、集中的に故障復旧を行う装置を設けることなく故障復旧を行うことができるATM通信網および故障復旧方法を提供することを目的とする。

【0007】

【課題を解決するための手段】単純な構成を持つ交換機を通信装置として適用するとき、交換機の故障時のVCルート障害を敏速に復旧する必要がある。そこで、本発明は、交換機の故障時にVCルート障害を敏速に復旧す

る方法を提供することを特徴とする。その方法としては交換機の故障時に、発着交換機間の現用ルート障害を復旧するために着交換機から故障復旧メッセージセルを送出し、交換機が自律分散的に情報を交換して発着交換機に網状態を通知し、ルートの切替えを行い、交換機故障によるルート障害がVCルートレベルにより復旧される。これをVCルートレベルのセルフヒーリングという。

【0008】従来技術では、VPレベルのセルフヒーリングが行われていたが、本発明の特徴とするところは、VCルートレベルのセルフヒーリングによって、交換機故障時のVCルート障害を復旧することができることにある。

【0009】すなわち、本発明の第一の観点は、複数の加入者交換機と、この複数の加入者交換機相互間を接続する複数の物理伝送路と、この複数の物理伝送路に介挿される中継交換機とを備え、前記複数の加入者交換機の間にバーチャルパスが設定されるATM通信網である。

【0010】ここで、本発明の特徴とするところは、前記加入者交換機には、バーチャルパスに故障復旧メッセージセルを送出する手段を備え、この故障復旧メッセージセルは、宛先領域およびメッセージ領域を有し、その宛先領域に一以上の中継交換機を経由して相手側の加入者交換機に到達するための情報が搭載され、前記中継交換機には、経由する前記故障復旧メッセージセルのメッセージ領域にその中継交換機の空帯域情報を搭載させる手段を備えたところにある。

【0011】前記メッセージ領域には、経由する中継交換機の数搭載するホップカウンタ領域が設けられ、前記中継交換機には、故障復旧メッセージセルが通過する毎にこのホップカウンタ領域に搭載された中継交換機の数を加算する手段を備えることが望ましい。

【0012】前記加入者交換機には、バーチャルパスに介挿された中継交換機の故障の可能性を認識する手段を備え、前記故障復旧メッセージセルを送出する手段は、この認識する手段の出力にしたがって故障復旧メッセージセルを送出することが望ましい。

【0013】前記加入者交換機には、複数のバーチャルパスを介して到来する故障復旧メッセージセルを受信する手段を備え、この故障復旧メッセージセルに含まれる空帯域情報および中継交換機の数にしたがって利用するバーチャルパスを選択する手段を備えることが望ましい。

【0014】本発明の第二の観点は故障復旧方法であり、その特徴とするところは、加入者交換機に設定されるバーチャルパスには現用のバーチャルパスおよび予備のバーチャルパスとなりうる複数のバーチャルパスがあらかじめ設定され、この現用のバーチャルパスに介挿される中継交換機に故障の可能性が認識されたとき、前記加入者交換機は故障復旧メッセージセルを前記予備のバーチャルパスとなりうる複数のバーチャルパスにそれぞ

れ送出し、この故障復旧メッセージセルの宛先となる加入者交換機では、この故障復旧メッセージセルに搭載された空帯域情報および中継交換機の数にしたがって前記予備のバーチャルパスとなりうる複数のバーチャルパスのいずれかを選択するところにある。

【0015】この故障復旧方法では、前記加入者交換機は一つの通信網の中に多数分散して存在し、各加入者交換機がこの故障復旧方法を自律分散的に実行することが特徴である。

【0016】本発明の第三の観点は故障復旧待機方法であり、その特徴とするところは、加入者交換機に設定されるバーチャルパスには現用のバーチャルパスおよび予備のバーチャルパスとなりうる複数のバーチャルパスがあらかじめ設定され、この現用のバーチャルパスに介挿される中継交換機の故障がなくても、前記加入者交換機は故障復旧メッセージセルを前記予備のバーチャルパスとなりうる複数のバーチャルパスにそれぞれ送出し、この故障復旧メッセージセルの宛先となる加入者交換機では、この故障復旧メッセージセルに搭載された空帯域情報および中継交換機の数にしたがって前記予備のバーチャルパスとなりうる複数のバーチャルパスのいずれかを予備のバーチャルパス候補としてあらかじめ選択するところにある。

【0017】この故障復旧待機方法では、前記加入者交換機は一つの通信網の中に多数分散して存在し、各加入者交換機がこの故障復旧待機方法を自律分散的に実行することが特徴である。

【0018】本発明の第四の観点は故障復旧方法であり、その特徴とするところは、一つの通信網内にある加入者交換機は自己にバーチャルパスを設定する自己およびまたはその通信網に属する他の加入者交換機に宛てて故障復旧メッセージセルをバーチャルパスにそれぞれ送し出すところにある。

【0019】この明細書では、加入者交換機と中継交換機とをあたかも異なる通信装置であるかのような表現を用いているが、これは説明をわかりやすくするためのものであり、同一のハードウェア構成の通信装置により実現することができる。

【0020】

【作用】本発明の方法では、V Cルートレベルのセルフヒーリングによって、着交換機から故障復旧メッセージセルを送出して、交換機が自律分散的に情報を交換し、発交換機に網状態を通知し、ルートの切替えを行い、交換機故障時のV Cルート障害を復旧することができるので、高信頼な交換機を使用する必然性がなくなり、単純な構成を持つ交換機を使用することにより、コスト削減が図られる。

【0021】着交換機が送し出す故障復旧メッセージセルはバーチャルパスを介して発交換機に到達する。このバーチャルパスは、予備のバーチャルパスとなりうるバ

ーチャルパスとしてあらかじめ定められているバーチャルパスでもよいし、故障が認識されていない不特定のバーチャルパスでもよい。

【0022】故障復旧メッセージセルは、着交換機から発交換機に到達する間に通過するバーチャルパスの空帯域情報を収集する。言い方を替えると、通過するバーチャルパスに介挿されている中継交換機は、故障復旧メッセージセルを通過させるときに、自己の中継交換機における空帯域情報を故障復旧メッセージセルの例えばメッセージ領域に搭載する。また、同時に通過した中継交換機の数も情報として搭載する。発交換機では、空帯域情報および通過した中継交換機の数情報を参考にして予備のバーチャルパスとして最適なバーチャルパスを選択する。以降は、このバーチャルパスにバーチャルチャンネルを設定して通信を再開する。

【0023】故障復旧メッセージセルの送し出は現用のバーチャルパスあるいは現用のバーチャルパス上の中継交換機に何らかの故障が認識されたときに行われるように制御してもよいし、あるいは、平常時にも故障復旧メッセージセルを送し出し、常時、予備のバーチャルパスとして最適なバーチャルパス候補を選択しておくこともよい。

【0024】本発明では、このような故障復旧制御をATM通信網に含まれる各交換機が自律分散に行うことを主要な特徴としている。

【0025】

【実施例】

(第一実施例) 本発明第一実施例の構成を図1～図5を参照して説明する。図1は本発明の全体構成図である。図2は着交換機の要部ブロック構成図である。図3は故障復旧メッセージセルの構成図である。図4は中継交換機の要部ブロック構成図である。図5は発交換機の要部ブロック構成図である。

【0026】本発明は、加入者交換機である発交換機1および着交換機6と、この発交換機1および着交換機6相互間を接続する物理伝送路P～Rと、この物理伝送路P～Rに介挿される中継交換機2、3、4、5、7、8、9とを備え、発交換機1および着交換機6の間にバーチャルパスが設定されるATM通信網である。

【0027】ここで、本発明の特徴とするところは、着交換機6には、バーチャルパスに故障復旧メッセージセルを送出する手段としての故障復旧メッセージセル生成部12を備え、この故障復旧メッセージセルは、宛先領域Hおよびメッセージ領域Mを有し、その宛先領域Hに一以上の中継交換機2、3、4、5、7、8、9を経由して発交換機1に到達するための情報が搭載され、中継交換機2、3、4、5、7、8、9には、経由する故障復旧メッセージセルのメッセージ領域Mにその中継交換機2、3、4、5、7、8、9の空帯域情報を搭載させる手段としての故障復旧メッセージセル情報搭載部14

を備えたところにある。

【0028】本発明実施例では、説明をわかりやすくするために、発交換機1、着交換機6、中継交換機2、3、4、5、7、8、9をそれぞれあたかも異なるハードウェア構成を備えた通信装置であるかのように表現するが、これらは各機能を共通に備えた一つの通信装置として実現することができる。

【0029】メッセージ領域Mには、経由する中継交換機2、3、4、5、7、8、9の数を搭載するホップカウンタ領域HCが設けられ、中継交換機2、3、4、5、7、8、9には、故障復旧メッセージセルが通過する毎にこのホップカウンタ領域HCに搭載された中継交換機の数を加算する手段を故障復旧メッセージセル情報搭載部14に併せて備えている。

【0030】発交換機1および着交換機6には、バーチャルパスに介挿された中継交換機2、3、4、5、7、8、9の故障の可能性を認識する手段としての故障検出部10を備え、故障復旧メッセージセル生成部12は、この故障検出部10の出力にしたがって故障復旧メッセージセルを送出する。

【0031】発交換機1には、複数のバーチャルパスを介して到来する故障復旧メッセージセルを受信する手段としての予備ルート設定部16を備え、この故障復旧メッセージセルに含まれる空帯域情報および中継交換機の数にしたがって利用するバーチャルパスを選択する手段を予備ルート設定部16に併せて備えている。

【0032】VCルートは発交換機1から1つ以上のVPを経て着交換機6に設定される。発交換機1において、呼が発生したときに、複数のVCルートの中からあるルートを選択して、呼受付判定(Connection Admission Control: CAC)を行う。例えば、ルートの選択は、ランダムに選択される。CACによって、呼が受け付けられたら、VCコネクションを設定し、呼が受け付けられなければ呼損となる。

【0033】次に、本発明第一実施例の動作を図6を参照して説明する。図6は本発明第一実施例の動作を説明するための図である。図6に示すように、1つの現用ルートのみに着目し、中継交換機5に故障が発生したときの、本発明第一実施例の故障回復方法を示す。発交換機1と着交換機6との間に現用ルート(1→4→5→6)が2つの中継交換機を介して設定されており、現用ルートは現時点でB(Mbps)の帯域を使用している。

【0034】この現用ルートに対して、CACの後に呼が受け付けられ、VCコネクションが設定されたり、切断されたりしている。この現用ルートの使用帯域は、例えば、発交換機1において、あるウィンドウサイズ内の現用ルートで使用されているセル数を観測することによって求められる。観測に使用されるウィンドウとして、ジャンピングウィンドウやスライディングウィンドウがある。

【0035】ここで、ジャンピングウィンドウとは、ウィンドウ位置(観測位置)が一定周期でオーバーラップすることなく遷移する観測方法であり、スライディングウィンドウとは、ウィンドウ位置が一定周期でオーバーラップしながら徐々に遷移する観測方法である。ごく大まかにいうとジャンピングウィンドウは高速な観測が利点であり、スライディングウィンドウは正確な観測が利点である。

【0036】故障により、現用ルートが使用不可能になることに備えて、複数の予備ルートを予め設定しておく。図6では、2つの予備ルート(ルートP: 1→2→3→6、ルートR: 1→7→8→9→6)が設定されている。故障が発生したとき、現用ルートが使用不可能な状態であることは、アラームを通知するセルその他により発交換機1および着交換機6が認識する。現用ルートに現時点で設定されていたVCコネクションの救済は行わないが、故障発生後に、新たに要求してくるVCの呼を最大限受けられるように、迂回ルートを探査する。ここで、着交換機6は故障復旧メッセージセルを送出するセンダ、発交換機1は故障復旧メッセージセルを受取り予備ルートの中から切替えルートを選択するチューザとなる。着交換機(センダ)6は、予備ルートに対してその状態を調べるために、故障復旧メッセージセルを送出する。故障復旧メッセージセルは予備ルートPおよびRの経路に沿って、予備ルートPおよびRの経路上のVPの状態を調べる。ルートRを例に上げて説明する。故障復旧メッセージセルのメッセージ領域Mにはペイロードとして、

- (1) ホップカウンタHC
- (2) ホップリミットHL
- (3) VP未使用帯域の最小値 b_{min}
- (4) 経路情報RD

が書込まれる。ホップリミットHLは、遅延条件その他を考慮して、予め設定されている。最小値 b_{min} の値を ∞ としておき、最小値 b_{min} の値は故障復旧メッセージセルに書込まれている。ルートRを経由する故障復旧メッセージセルは、着交換機6から中継交換機9に送出され、中継交換機9では、 $b < b_{min}$

ならば、未使用VP帯域 b の値を b_{min} とする。 b は中継交換機9において、例えば、あるウィンドウサイズ内のVP未使用帯域は、使用セル数を観測することによって求められる。観測に使用されるウィンドウとして、ジャンピングウィンドウやスライディングウィンドウがある。ホップカウンタHCは中継交換機9→8→7を経由する毎に、1つカウントアップされ、ホップリミットHLを超えない限り、さらに次の交換機に送出される。しかし、通常、予備ルートは、ホップリミットを超えないように予め設定されている。次の交換機8では、 $b = 2$ であり、 $b < b_{min}$ なので、 $b_{min} = 2$ となる。同様に

故障復旧メッセージセル送出手続きを繰り返し、故障復旧メッセージセルは、発交換機1に到着する。また、予備ルートP上に送出された故障復旧メッセージセルAも同様にして、発交換機1に到着する。発交換機1は、予備ルートPまたはRの中から、現用ルートの使用帯域Bや予備ルート情報（VP未使用帯域の最小値 b_{min} 、ホップ数）その他を考慮して、切替先のルートとして1つまたは複数選択する。図7は本発明第一実施例におけるルート切替状況を示す図であるが、図7の例では、予備ルートの中でルートPが最もVP未使用帯域の最小値が大きいため、ルートPが切替先のルートとして選択され、故障復旧後はルートPが現用ルートとして使用される。

【0037】したがって、交換機の故障時に、故障復旧メッセージセルの送出により交換機が自律分散的に情報を交換し、ルートの切替えを行い、故障が復旧されるので、従来のような2重化された高信頼な交換機でなくても単純な構成を持つ交換機を用いることができるため、交換機のコスト削減が図れる。

【0038】（第二実施例）次に、本発明第二実施例を 図8を参照して説明する。図8は本発明第二実施例の動作を説明するための図である。本発明第一実施例では、故障発生時に故障復旧メッセージセルを送出していたが、本発明第二実施例では、図8のように、通常時でも、着交換機（センダ）6からRM(Resource Management)セルを送出して、予備ルートPおよびRの状態を監視しておく。RMセルの動作は、本発明第一実施例の故障復旧メッセージセルの動作と同様である。発交換機（チューザ）1は、予備ルートPまたはRの中から、現用ルートの使用帯域Bや予備ルート情報（VP未使用帯域の最小値 b_{min} 、ホップ数）その他を考慮して、現用ルートの障害時に備えて、切替先のルートを決めておく。

【0039】ここで、着交換機（センダ）6からRMセルは、定期的に送出され、RMセルを受け取った発交換機（チューザ）1は、網状態に応じて切替先のルートを更新しておく。RMセルの送出間隔は、網状態の変化の度合いから決定される。

【0040】故障が発生したとき、現用ルートが使用不可能な状態であることは、アラームを通知するセルその他により発交換機1が認識する。現用ルートの障害を検知した発交換機1は、通常に現用ルート障害時に備えてあった切替先ルートに切替えられ、現用ルートとして使用される。

【0041】したがって、通常時に、着交換機（センダ）6からRM(Resource Management)セルを送出して、予備ルートの状態を監視して、現用ルートの障害時に備えて切替先ルートを決めておくことにより、故障復旧時間の短縮化が図れる。

【0042】（第三実施例）次に、本発明第三実施例を

図9を参照して説明する。図9は本発明第三実施例の動作を説明するための図である。本発明第一実施例では、予め予備ルートPおよびRを設定しておき、故障発生時に予備ルートPおよびR上に故障復旧メッセージセルを送出していた。本発明第三実施例では、予め予備ルートPおよびRを設定しておかず、図9のようにフラッディング(Flooding)により故障復旧メッセージセルを送出し、発交換機1に到達した故障復旧メッセージセルにしたがって発交換機1が予備ルートを選択する。

【0043】ここで、フラッディングとは、“Flood”すなわち、あたかも“洪水”のように不特定方向に対してセルを送出させるというイメージに基づいた用語であり、自交換機へVPを送出するすべての交換機へ故障復旧メッセージセルを送出するという意味に用いる。

【0044】故障復旧メッセージセルのペイロードには、本発明第一実施例で説明したように、

- (1) ホップカウンタHC
- (2) ホップリミットHL
- (3) VP未使用帯域の最小値 b_{min}
- (4) 経路情報RD

が書込まれる。ホップリミットHLは、遅延条件その他を考慮して、予め設定されている。最小値 b_{min} の値を ∞ としておき、最小値 b_{min} の値は故障復旧メッセージセルに書込まれている。

【0045】まず、着交換機（センダ）6は、自交換機へVPを送出するすべての交換機へ故障復旧メッセージセルを送出する。故障復旧メッセージセルを受信した交換機は、 $b < b_{min}$ ならば、未使用VP帯域 b の値を b_{min} とする。 b は交換機において、例えば、あるウィンドウサイズ内のVP未使用帯域は、使用セル数を観測することによって求められる。経路した交換機の情報が経路情報として書込まれる。ホップカウンタHCは交換機を経由する毎に、1つカウントアップされ、もし、ホップリミットHLを超えているか、または、経路情報RDにより既に同じ交換機を経由していれば、故障復旧メッセージセルは廃棄される。そうでなければ、さらに、自交換機へVPを送出するすべての交換機へ故障復旧メッセージセルを送出し、故障復旧メッセージセルを受信した交換機は同様の動作を繰り返し、故障復旧メッセージセルは、発交換機に到着する。

【0046】発交換機（チューザ）1は、到着した故障復旧メッセージセルから現用ルートの使用帯域Bや到着した故障復旧メッセージセルを基にしたルート情報（VP未使用帯域の最小値 b_{min} 、ホップ数）その他を考慮して、切替先のルートとして1つまたは複数選択する。

【0047】したがって、予め予備ルートを設定しておくことなく、フラッディングにより故障復旧メッセージセルを送出し、発交換機1に故障復旧メッセージセルを到着させることにより、網トポロジやVP容量その他の変化に柔軟に対応した故障復旧を行うことができる。

【0048】本発明の故障復旧方法による故障復旧概念を図10および図11に示す。図10は本発明の故障復旧方法の概念を示す図である。図11は本発明の故障復旧方法を適用したATM通信網の概念図である。図10(b)および(c)は、従来から知られているVPレベルおよび物理レベルの故障復旧概念である。本発明では図10(a)に示すように、VCルートレベルの故障復旧を行うことにより図11に示すように、高信頼性の交換機を用いることなくATM通信網を構成することができる。

【0049】

【発明の効果】以上説明したように、本発明によれば、交換機の故障を前提とした故障復旧制御を行うことができる。このため、交換機の高信頼性を確保するための冗長なハードウェア構成を省略することができる。したがって、交換機のコストを低減することができる。さらに、集中的に故障復旧を行う装置を設けることなく故障復旧を行うことができる。

【図面の簡単な説明】

【図1】本発明の全体構成図。

【図2】着交換機の要部ブロック構成図。

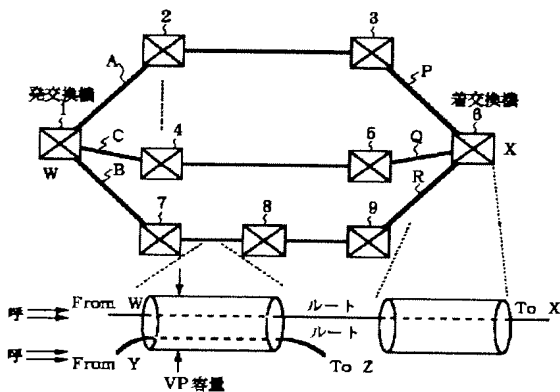
【図3】故障復旧メッセージセルの構成図。

【図4】中継交換機の要部ブロック構成図。

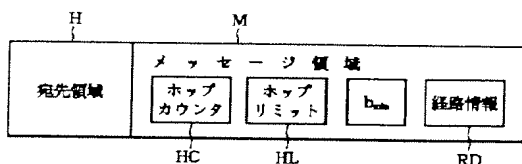
【図5】発交換機の要部ブロック構成図。

【図6】本発明第一実施例の動作を説明するための図。

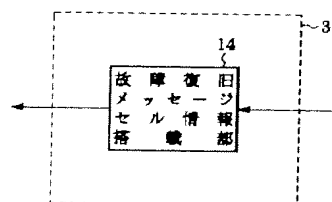
【図1】



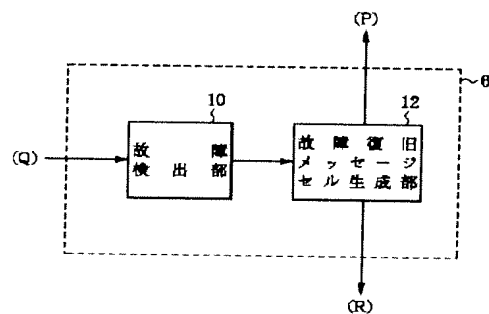
【図3】



【図4】



【図2】



【図7】本発明第一実施例におけるルート切替状況を示す図。

【図8】本発明第二実施例の動作を説明するための図。

【図9】本発明第三実施例の動作を説明するための図。

【図10】本発明の故障復旧方法の概念を示す図。

【図11】本発明の故障復旧方法を適用したATM通信網の概念図。

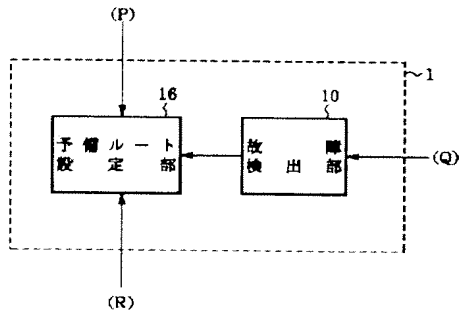
【図12】従来の故障復旧方法の概念を示す図。

【図13】高信頼化された交換機の概念図。

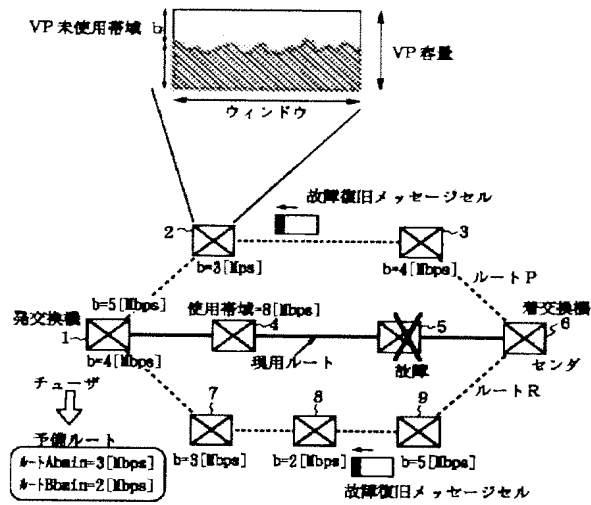
10 【符号の説明】

- 1 発交換機
- 2~5、7~9 中継交換機
- 6 着交換機
- 10 故障検出部
- 12 故障復旧メッセージセル生成部
- 14 故障復旧メッセージセル情報搭載部
- 16 予備ルート設定部
- H 宛先領域
- HC ホップカウンタ
- HL ホップリミット
- M メッセージ領域
- RD 経路情報
- b_{min} 最小値
- P、Q、R ルート

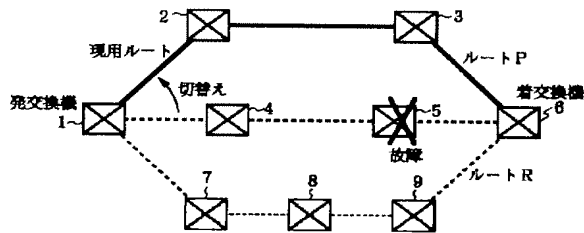
【図5】



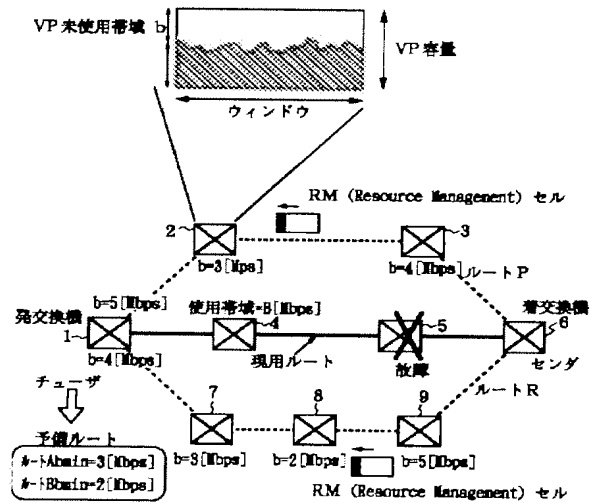
【図6】



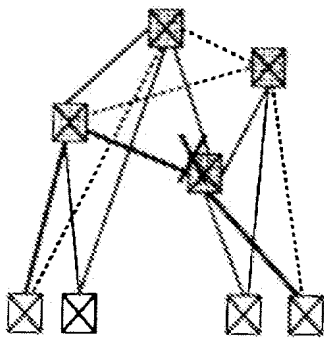
【図7】



【図8】

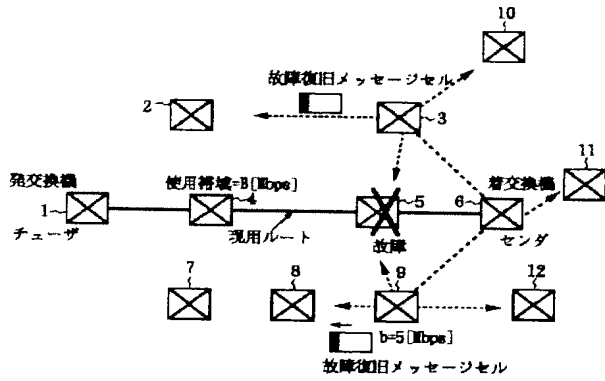


【図11】

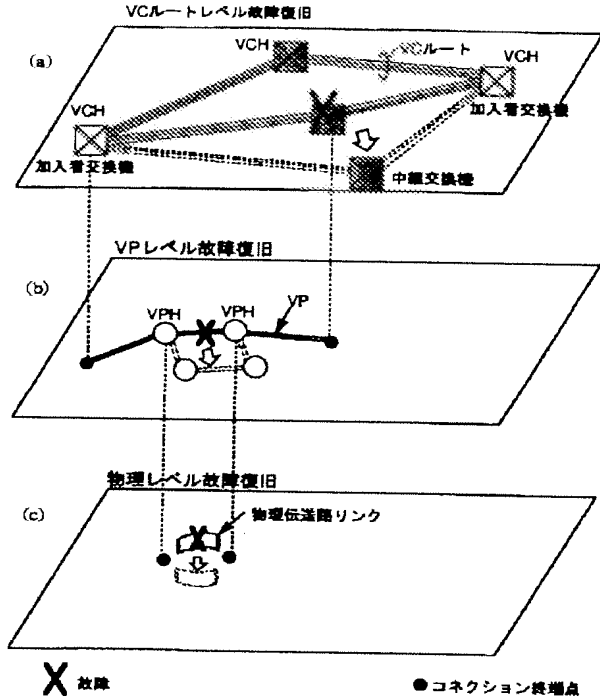


交換機のダウンサイジング化

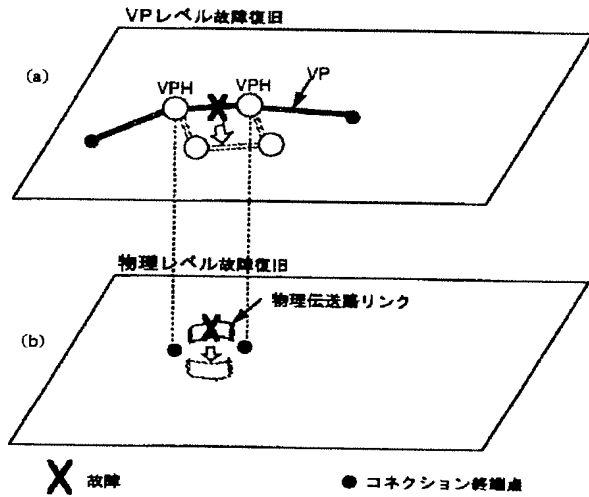
【図9】



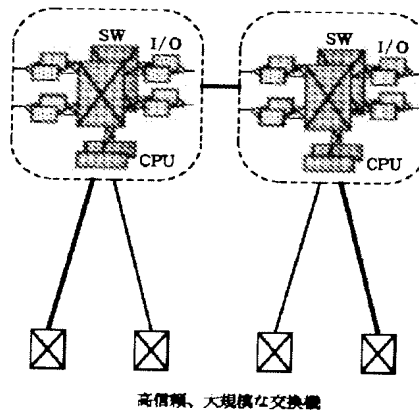
【図10】



【図12】



【図13】



Electronic Patent Application Fee Transmittal

Application Number:	11839987
Filing Date:	16-Aug-2007
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Atabak R Royae/Melissa Molchan
Attorney Docket Number:	77580-0066 (VRNK-1 CP2DVCN)

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	810	810
Total in USD (\$)				810

Electronic Acknowledgement Receipt

EFS ID:	7342654
Application Number:	11839987
International Application Number:	
Confirmation Number:	9470
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Atabak R Royaee/Melissa Molchan
Filer Authorized By:	Atabak R Royaee
Attorney Docket Number:	77580-0066 (VRNK-1CP2DVCN)
Receipt Date:	02-APR-2010
Filing Date:	16-AUG-2007
Time Stamp:	14:15:49
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$810
RAM confirmation Number	364
Deposit Account	501133
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	-------------------------------------	------------------	------------------

1		0066.pdf	129407 2c4c3f0f6109cdbc093c043eaeff4448f23f773e	yes	5
Multipart Description/PDF files in .zip description					
		Document Description	Start	End	
		Request for Continued Examination (RCE)	1	2	
		Information Disclosure Statement (IDS) Filed (SB/08)	3	5	
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
2		jp.pdf	2159740 c1f5c3a6d9721ee83f8ef0087e759d448898a69	yes	53
Multipart Description/PDF files in .zip description					
		Document Description	Start	End	
		Foreign Reference	1	6	
		Foreign Reference	7	23	
		Foreign Reference	24	30	
		Foreign Reference	31	53	
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
3	NPL Documents	Feng.pdf	215626 58bf05014b12aa13483ab383b6d7b0c529b2e711	no	4
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
4	NPL Documents	Davies.pdf	572855 570f1932ebcd625d840e44ae1e6c1c78603cf33c	no	15
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					

5	Fee Worksheet (PTO-875)	fee-info.pdf	30849 989366f95befb6eeae95071997668f0dc80c8d8	no	2
---	-------------------------	--------------	--	----	---

Warnings:

Information:

Total Files Size (in bytes):	3108477
-------------------------------------	---------

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

Table with columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO., EXAMINER, ART UNIT, PAPER NUMBER, NOTIFICATION DATE, DELIVERY MODE. Includes application details for Victor Larson and examiner LIM, KRISNA.

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. 11/839,987	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 --

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 02 April 2010.
- 2a) This action is **FINAL**.
- 2b) This action is non-final.
- 3) 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

- 4) Claim(s) 1-18 is/are pending in the application.
 - 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-18 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) 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).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 - 1. Certified copies of the priority documents have been received.
 - 2. Certified copies of the priority documents have been received in Application No. _____.
 - 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

Art Unit: 2453

Claims 1-18 are still pending for examination.

As required by M.P.E.P. 609(C), the applicant's submissions of the Information Disclosure Statement dated April 02, 2010 is acknowledged by the examiner and the cited references have been considered in the examination of the claims now pending. As required by M.P.E.P. 609 C(2), a copy of the PTOL-1449 initialed and dated by the examiner is attached to the instant office action..

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).

Claims 1-18 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 2-23 of copending Application No.

Art Unit: 2453

11/679,416. Although the conflicting claims are not identical, they are not patentably distinct from each other because a method of accessing a secure computer network address (i.e., a method of communicating with a device having a secure name), comprising steps of: a) sending a query message to a secure domain service ...; b) receiving from the secure domain name service ...; and c) sending an access request message ... to the address using a secure communication link.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-18 are rejected under 35 U.S.C. § 103(a) as being unpatentable over VPN Overview and Aventail connect v3.1/v2.6 administrator's Guide References (hereafter VPN Overview and/or Aventail). Applicants submitted these papers.

Aventail disclosed the invention substantially as claimed. Taking claim 1 as exemplary claims, the reference discloses a method of accessing a secure network (e.g., see pages 6, 12, 46, 62 and 66 for the teaching of "security firewall", "enabling remote users to gain secure access to internal network resources", etc.), comprising:

 sending a query message from a first network device to a secure domain service, the query message requesting from the secure domain service_a secure network address for a second network device (e.g., see page 8, 12, 45 and 48 for the teaching of Domain Name System lookup to convert the hostname to an IP address,

 receiving at the first network device a response message from the secure domain

Art Unit: 2453

name service containing the secure network address for the second network device (e.g. see page 8 for the teaching of DNS lookup to convert the hostname into an IP address and vice versa, and see page 12 for the teaching of SOCKS negotiation when the connection is completed); and

 sending an access request message from the first network device to the secure network address using a virtual private network communication link (e.g. see page 6 for the teaching of safeguard corporate networks and the exchanged information, and on pages 8 and 12 for the teaching of the application requests a connection to the specified remote host... the handshake between two computers).

As to claim 2, Aventail further disclosed supporting a plurality of services over the virtual private network communication link (e.g., see page 116 for VPN: a secure channel used to transmit data over a public network, page 77 for VPN communication link).

As to claim 3, Aventail further disclosed the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or any combination thereof (e.g., at page 68, Aventail Connect can open connections through SOCKS servers, through HTTP proxies, or through proxy chaining, and the teaching of TCP/IP in page 11-12).

As to claim 4, the feature of a plurality of application programs comprises video conferencing, e-mail, a word processing program, telephony or any combination thereof is well known in the art at the time the invention was made.

As to claim 5, the feature of a plurality of services comprises audio, video, or any combination thereof is well known in the art at the time the invention was made.

As to claim 6, Aventail further disclosed the secure network address includes a security feature (e.g. see page 6 for the teaching of security firewalls, and page 46 for the teaching of SOCKS v5 servers that often require user authentication before allowing

Art Unit: 2453

access, the teaching of authentication module).

As to claim 7, Aventail further disclosed the secure network address is encrypted (e.g., see pages 7, 10, 29, 46, 55, 68 and 77).

As to claim 8, Aventail further disclosed decrypting the encrypted secure network address (e.g., see pages 7, 10, 29, 46, 55, 68 and 77).

As to claim 9, Aventail further disclosed supporting an un-secure communication link between the first and second network device (e.g. see page 29 for the teaching of Aventail allows user to select any, all or none of authentication modules and in versions of Aventail Connect that do not include encryption, the secure Sockets Layer).

As to claim 10, Aventail further disclosed the secure network address is an IP address belonging to the second network device (e.g. see the teaching of "How Does Aventail Connect Work?" on pages 11 and 12).

As to claim 11, Aventail further disclosed automatically initiating the virtual private network communication link after the access request message is received at the second network device (e.g., see page 116 for VPN: a secure channel used to transmit data over a public network, page 77 for VPN communication link).

As to claim 12, Aventail further disclosed using tunneling (e.g. see page 7 for the teaching of establishing an encrypted tunnel automatically) over the virtual private network communication link.

As to claim 13, Aventail further disclosed using tunnel packeting over the virtual private network communication link (e.g. see page 7 for the teaching of establishing an encrypted tunnel automatically).

Art Unit: 2453

As to claim 14, Aventail further disclosed the secure communication link is an authenticated link (e.g. see authentication module on pages 6, 12, 29, 34 and 46).

As to claim 15, Aventail further disclosed with a client computer connected to a communication network (e.g. see Aventail connect client connected to Internet on pages 77 and 79).

As to claim 16, Aventail further disclosed the second network device has an unsecure name (e.g. see page 29 for the teaching of Aventail allows user to select any, all or none of authentication modules and in versions of Aventail Connect that do not include encryption, the secure Sockets Layer, and on page 48 for the teaching of Disable/Enable authentication modules).

As to claim 17, Aventail further disclosed the secure network address is registered with the secure domain service prior to the step of sending a query message to a secure domain service (see the teaching of define destination with IP address, subset and address ranges on pages 40-41).

As to claim 18, Aventail further disclosed with a mobile device connected to a communication network through a cellular network (e.g., see Mobile VPN on page 77).

As mention above, Aventail disclosed both DNS request and VPN establish. Aventail did not explicitly detail the VPN. Such detail VPN (e.g., see Figs. 1-3 and 9, pages 6, 9, 11-12, 15, 22-28, etc.) is clearly taught by VPN Overview. Thus, it would have been obvious to one of ordinary skilled in the art to combine the teaching of Aventail with the well known VPN (e.g., VPN Overview) so that the system with the feature of enhanced security, effectively monitoring and directing network traffic would be archived as suggested by Aventail (e.g., see page 1).

Art Unit: 2453

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, Joseph Thomas, can be reached on 571-272-6776. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.


Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KI

July 4, 2010

/Krisna Lim/

Primary Examiner, Art Unit 2453

Index of Claims 	Application/Control No. 11839987	Applicant(s)/Patent Under Reexamination LARSON ET AL.
	Examiner Krisna Lim	Art Unit 2453

✓	Rejected
=	Allowed


-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

Claims renumbered in the same order as presented by applicant
 CPA
 T.D.
 R.1.47

CLAIM		DATE							
Final	Original	06/05/2009	12/29/2009	02/13/2010	07/04/2010				
	1	✓	✓	=	✓				
	2		○	=	✓				
	3		○	=	✓				
	4		○	=	✓				
	5		○	=	✓				
	6		○	=	✓				
	7		○	=	✓				
	8		○	=	✓				
	9		○	=	✓				
	10		○	=	✓				
	11		○	=	✓				
	12		○	=	✓				
	13		○	=	✓				
	14		○	=	✓				
	15		○	=	✓				
	16		○	=	✓				
	17		○	=	✓				
	18		○	=	✓				

Search Notes 	Application/Control No. 11839987	Applicant(s)/Patent Under Reexamination LARSON ET AL.
	Examiner Krisna Lim	Art Unit 2453

SEARCHED			
Class	Subclass	Date	Examiner
709	225-229, 245	2/13/2010	kl
726	15	2/13/2010	kl

SEARCH NOTES		
Search Notes	Date	Examiner
EAST, Inventors	2/13/2010	kl

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner
709	227, 228	2/13/2010	kl

--	--

Subst. for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Application Number	11/839,987
				Filing Date	08/16/2007
				First Named Inventor	Victor Larson
				Art Unit	2453
				Examiner Name	Krisna Lim
				Docket Number	077580-0066
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
	A1	5,764,906	06/1998	Edelstein et al.	
	A2	5,864,666	01/1999	Shrader, Theodore Jack London	
	A3	5,898,830	04/1999	Wesinger et al.	
	A4	6,052,788	04/2000	Wesinger et al.	
	A5	6,061,346	05/2000	Nordman, Mikael	
	A6	6,081,900	06/2000	Subramaniam et al.	
	A7	6,101,182	08/2000	Sistanizadeh et al.	
	A8	6,199,112	03/2001	Wilson, Stephen K.	
	A9	6,202,081	03/2001	Naudus, Stanley T.	
	A10	6,298,341	10/2001	Mann et al.	
	A11	6,262,987	07/2001	Mogul, Jeffrey C.	
	A12	6,314,463	11/2001	Abbott et al.	
	A13	6,338,082	01/2002	Schneider, Eric	
	A14	6,502,135	12/2002	Munger et al.	
	A15	6,557,037	04/2003	Provino, Joseph E.	
	A16	6,687,746	02/2004	Shuster et al.	
	A17	6,757,740	06/2004	Parkh et al.	
	A18	7,039,713	05/2006	Van Gunter et al.	
	A19	7,167,904	01/2007	Devarajan et al.	
	A20	7,188,175	03/2007	McKeeth, James A.	
	A21	7,461,334	12/2008	Lu et al.	
	A22	7,490,151	02/2009	Munger et al.	
	A23	7,493,403	02/2009	Shull 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
	B1	US2001/0049741	12/2001	Skene et al.	
	B2	US2004/0199493	10/2004	Ruiz et al.	
	B3	US2004/0199520	10/2004	Ruiz et al.	
	B4	US2004/0199608	10/2004	Rechterman et al.	
	B5	US2004/0199620	10/2004	Ruiz et al.	
	B6	US2007/0208869	09/2007	Adelman et al.	
	B7	US2007/0214284	09/2007	King et al.	

Subst. for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Application Number	11/839,987
				Filing Date	08/16/2007
				First Named Inventor	Victor Larson
				Art Unit	2453
				Examiner Name	Krisna Lim
				Docket Number	077580-0066

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
	B8	US2007/0266141	11/2007	Norton, Michael Anthony	
	B9	US2008/0235507	09/2008	Ishikawa et al.	

FOREIGN PATENT DOCUMENTS							
EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes-Number + -Kind Codes (if known)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No
	C1	JP04-363941	12/16/1992	Nippon Telegr & Teleph Corp	English Abstract		
	C2	JP09-018492	01/17/1997	Nippon Telegr & Teleph Corp	English Abstract		
	C3	JP10-070531	03/10/1998	Brother Ind Ltd.	English Abstract		
	C4	JP62-214744	9/21/1987	Hitachi Ltd.	English Abstract		

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	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)	
	D2	D.W. Davies and W.L. Price, edited by Tadahiro Uezono, "Network Security", Japan, Nikkei McGraw-Hill, December 5, 1958, First Edition, first copy, p. 102-108	
EXAMINER		/Krisna Lim/	DATE CONSIDERED 07/02/2010

*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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known			
				Application Number		11/839,987	
				Filing Date		August 16, 2007	
				First Named Inventor		Victor Larson	
				Art Unit		2453	
				Examiner Name		LIM, Krisna	
Sheet	1	of	2	Docket Number	077580-0066 (VRNK-1CP2DVCN2)		
U.S. PATENT DOCUMENTS							
EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code ² (if known)	Publication Date MM-DD-YYYY	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 Code ³ -Number ⁴ -Kind Codes (if known)	Publication Date MM-DD-YYYY	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.					
	C1227	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					
	C1228	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					
	C1229	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					
	C1230	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					
	C1231	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					
EXAMINER /Krisna Lim/				DATE CONSIDERED 02/13/2010			

*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 SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Complete if Known		
				Application Number	11/839,987	
				Filing Date	August 16, 2007	
				First Named Inventor	Victor Larson	
				Art Unit	2453	
Sheet	2	of	2	Examiner Name	LIM, Krisna	
OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)						
	C1232	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				
	C1233	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				
	C1234	Derrell Piper, "The Internet IP Security Domain of Interpretation for ISAKMP," RFC 2407 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html				
	C1235	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				
	C1236	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				
	C1237	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				
	C1238	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				
	C1239	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")				
EXAMINER				DATE CONSIDERED		
/Krisna Lim/				02/13/2010		

*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.

BST99 1640187-1.077580.0066

Subst. for form 1449/PTO SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Complete if Known		
				Application Number	11/839,987	
				Filing Date	August 16, 2007	
				First Named Inventor	Victor Larson	
				Art Unit	2453	
Examiner Name	LIM, Krisna					
Sheet	1	of	1	Docket Number	077580-0066 (VRNK-1CP2DVCN2)	

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code ₂ (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1019	US 7,461,334	12/02/08	Lu, et al.	
	A1020	US 7,353,841	04/08/08	Kono, et al.	
	A1021	US 7,188,175	03/06/07	McKeeth, James A.	
	A1022	US 7,167,904	01/23/07	Devarajan, et al.	
	A1023	US 7,039,713	05/02/06	Van Gunter, et al.	
	A1024	US 6,757,740	06/29/04	Parekh, et al.	
	A1025	US 6,752,166	06/22/04	Lull, et al.	
	A1026	US 6,687,746	02/03/04	Shuster, et al.	
	A1027	US 6,338,082	01/08/02	Schneider, Eric	
	A1028	US 6,333,272	12/25/01	McMillin, et al.	
	A1029	US 6,314,463	11/06/01	Abbott, et al.	
	A1030	US 6,298,341	10/02/01	Mann, et al.	
	A1031	US 6,262,987	07/17/01	Mogul, Jeffrey C.	
	A1032	US 6,199,112	03/06/04	Wilson, Stephen K.	
	A1033	US 2,895,502	07/21/59	Garland Roper Charles, et al.	
	A1034	US 2001/0049741	12/06/01	Skene, et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code ₃ -Number 4-Kind Codes (if known)	Publication Date MM-DD-YYYY	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.
	C1240	David Kosiur, "Building and Managing Virtual Private Networks" (1998)
	C1241	P. Mockapetris, "Domain Names - Implementation and Specification," Network Working Group, RFC 1035 (November 1987)
	C1242	Request for Inter Partes Reexamination of Patent No. 6,502,135, dated Nov. 25, 2009.
	C1243	Request for Inter Partes Reexamination of Patent No. 7,188,180, dated Nov. 25, 2009.

EXAMINER /Krisna Lim/	DATE CONSIDERED 02/13/2010
-----------------------	----------------------------

*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.

BST99 1640184-1.077580.0066

077580-0057 Subst. for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Application Number	11/839,987
				Filing Date	08/16/2007
				First Named Inventor	Victor Larson
				Art Unit	2453
				Examiner Name	Krisna Lim
				Docket Number	077580-0066

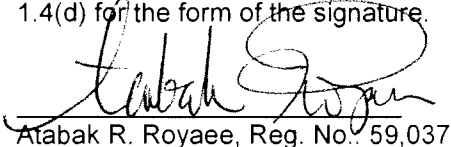
CERTIFICATION STATEMENT

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

- Information Disclosure Statement is being filed before the receipt of a first office action.
- Items contained in this Information Disclosure Statement were first cited in any communication from a foreign patent office in a counterpart foreign application.
- No item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned, after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of this Information Disclosure Statement
- The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of \$180.00, or further fees which may be due, to Deposit Account 50-1133.
- Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of \$810.00, or further fees which may be due, to Deposit Account 50-1133.
- None

SIGNATURE

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



Atabak R. Royae, Reg. No.: 59,037
 McDermott Will & Emery LLP
 28 State Street
 Boston, MA 02108
 Tel. (617) 535-4000
 Fax (617) 535-3800

Date: August 3, 2010

BST99 1655108-1.077580.0066

Subst. for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Application Number	11/839,987
				Filing Date	08/16/2007
				First Named Inventor	Victor Larson
				Art Unit	2453
				Examiner Name	Krisna Lim
				Docket Number	077580-0066

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
	A1019	5,870,610	02/1999	Beyda et al.	

FOREIGN PATENT DOCUMENTS

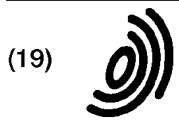
EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes -Number + -Kind Codes (if known)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No
	B1003	EP0838930	4/29/1988	Digital Equipment Corporation			
	B1004	EP0814589	12/29/1997	AT&T Corp.			
	B1005	GB2317792	04/01/1998	Secure Computing Corporation			
	B1006	WO98/27783	06/25/1998	Northern Telecom Limited			
	B1007	WO99/11019	03/04/1999	V One Corp			
	B1008	GB2334181	08/11/1999	NEC Technologies			
	B1009	GB2340702	02/23/2000	Sun Microsystems Inc.			

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.
	C1244	Baumgartner et al, "Differentiated Services: A New Approach for Quality of Service in the Internet," International Conference on High Performance Networking, 255-273 (1998)
	C1245	Chapman et al., "Domain Name System (DNS)," 278-296 (1995)
	C1246	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)
	C1247	De Raadt et al., "Cryptography in OpenBSD," 10 pages (1999)
	C1248	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)

Subst. for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Application Number	11/839,987
				Filing Date	08/16/2007
				First Named Inventor	Victor Larson
				Art Unit	2453
				Examiner Name	Krisna Lim
				Docket Number	077580-0066

	C1249	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)	
	C1250	Shimizu, "Special Feature: Mastering the Internet with Windows 2000", Internet Magazine, 63:296-307 (2000)	
	C1251	Stallings, "Cryptography and Network Security," Principals and Practice, 2nd Edition, pages 399-440 (1999)	
	C1252	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)	
	C1253	Wells, Email (Lancasterb1be@mail.msn.com), Subject: "Security Icon," (1998)	



Europäisches Patentamt
 European Patent Office
 Office européen des brevets



(11) EP 0 838 930 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
 29.04.1998 Bulletin 1998/18

(51) Int. Cl.⁶: H04L 29/06

(21) Application number: 97118556.6

(22) Date of filing: 24.10.1997

(84) Designated Contracting States:
 AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC
 NL PT SE
 Designated Extension States:
 AL LT LV RO SI

(72) Inventors:
 • Alden, Kenneth F.
 Boylston, Massachusetts 01505 (US)
 • Lichtenberg, Mitchell P.
 Sunnyvale, CA 94087 (US)
 • Wobber, Edward P.
 Menlo Park, California 94025 (US)

(30) Priority: 25.10.1996 US 738155

(71) Applicant:
 DIGITAL EQUIPMENT CORPORATION
 Maynard, Massachusetts 01754 (US)

(74) Representative: Betten & Resch
 Reichenbachstrasse 19
 80469 München (DE)

(54) Pseudo network adapter for frame capture, encapsulation and encryption

(57) A new pseudo network adapter provides an interface for capturing packets from a local communications protocol stack for transmission on the virtual private network, and includes a Dynamic Host Configuration Protocol (DHCP) server emulator, and an Address Resolution Protocol (ARP) server emulator. The new system indicates to the local communications protocol stack that nodes on a remote private network are reachable through a gateway that is in turn reachable through the pseudo network adapter. A transmit path in the system processes data packets from the local communications protocol stack for transmission through the pseudo network adapter. An encryption engine encrypts the data packets and an encapsulation engine encapsulates the encrypted data packets into tunnel data frames. The network adapter further includes an interface into a transport layer of the local communications protocol stack for capturing received data packets from the remote server node, and a receive path for processing received data packets captured from the transport layer of the local communications protocol stack. The receive path includes a decapsulation engine, and a decryption engine, and passes the decrypted, decapsulated data packets back to the local communications protocol stack for delivery to a user.

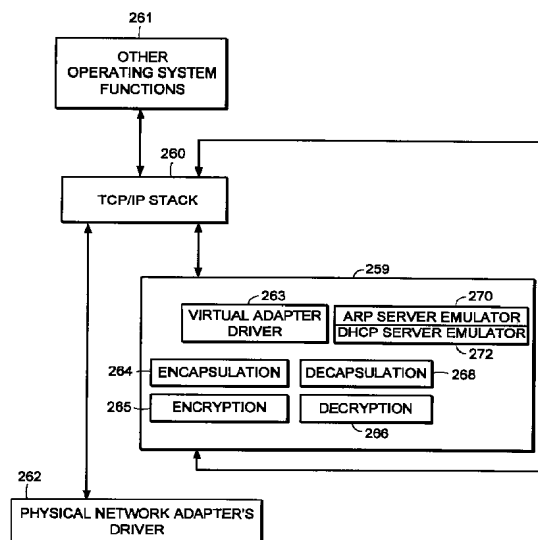


FIG. 15

EP 0 838 930 A2

Description**FIELD OF THE INVENTION**

The invention relates generally to establishing secure virtual private networks. The invention relates specifically to a pseudo network adapter for capturing, encapsulating and encrypting messages or frames.

BACKGROUND

In data communications it is often required that secure communications be provided between users of network stations (also referred to as "network nodes") at different physical locations. Secure communications must potentially extend over public networks as well as through secure private networks. Secure private networks are protected by "firewalls", which separate the private network from a public network. Firewalls ordinarily provide some combination of packet filtering, circuit gateway, and application gateway technology, insulating the private network from unwanted communications with the public network.

One approach to providing secure communications is to form a virtual private network. In a virtual private network, secure communications are provided by encapsulating and encrypting messages. Encapsulated messaging in general is referred to as "tunneling". Tunnels using encryption may provide protected communications between users separated by a public network, or among a subset of users of a private network.

Encryption may for example be performed using an encryption algorithm using one or more encryption "keys". When an encryption key is used, the value of the key determines how the data is encrypted and decrypted. When a public-key encryption system is used, a key pair is associated with each communicating entity. The key pair consists of an encryption key and a decryption key. The two keys are formed such that it is unfeasible to generate one key from the other. Each entity makes its encryption key public, while keeping its decryption key secret. When sending a message to node A, for example, the transmitting entity uses the public key of node A to encrypt the message, and then the message can only be decrypted by node A using node A's private key.

In a symmetric key encryption system a single key is used as the basis for both encryption and decryption. An encryption key in a symmetric key encryption system is sometimes referred to as a "shared" key. For example, a pair of communicating nodes A and B could communicate securely as follows: a first shared key is used to encrypt data sent from node A to node B, while a second shared key is to be used to encrypt data sent from node B to node A. In such a system, the two shared keys must be known by both node A and node B. More examples of encryption algorithms and keyed encryption are disclosed in many textbooks, for example

"Applied Cryptography - Protocols, Algorithms, and Source Code in C", by Bruce Schneier, published by John Wiley and Sons, New York, New York, copyright 1994.

Information regarding what encryption key or keys are to be used, and how they are to be used to encrypt data for a given secure communications session is referred to as "key exchange material". Key exchange material may for example determine what keys are used and a time duration for which each key is valid. Key exchange material for a pair of communicating stations must be known by both stations before encrypted data can be exchanged in a secure communications session. How key exchange material is made known to the communicating stations for a given secure communications session is referred to as "session key establishment".

A tunnel may be implemented using a virtual or "pseudo" network adapter that appears to the communications protocol stack as a physical device and which provides a virtual private network. A pseudo network adapter must have the capability to receive packets from the communications protocol stack, and to pass received packets back through the protocol stack either to a user or to be transmitted.

A tunnel endpoint is the point at which any encryption/decryption and encapsulation/decapsulation provided by a tunnel is performed. In existing systems, the tunnel end points are pre-determined network layer addresses. The source network layer address in a received message is used to determine the "credentials" of an entity requesting establishment of a tunnel connection. For example, a tunnel server uses the source network layer address to determine whether a requested tunnel connection is authorized. The source network layer address is also used to determine which cryptographic key or keys to use to decrypt received messages.

Existing tunneling technology is typically performed by encapsulating encrypted network layer packets (also referred to as "frames") at the network layer. Such systems provide "network layer within network layer" encapsulation of encrypted messages. Tunnels in existing systems are typically between firewall nodes which have statically allocated IP addresses. In such existing systems, the statically allocated IP address of the firewall is the address of a tunnel end point within the firewall. Existing systems fail to provide a tunnel which can perform authorization based for an entity which must dynamically allocate its network layer address. This is especially problematic for a user wishing to establish a tunnel in a mobile computing environment, and who requests a dynamically allocated IP address from an Internet Service Provider (ISP).

Because existing virtual private networks are based on network layer within network layer encapsulation, they are generally only capable of providing connectionless datagram type services. Because datagram type services do not guarantee delivery of packets, existing

tunnels can only easily employ encryption methods over the data contained within each transmitted packet. Encryption based on the contents of multiple packets is desirable, such as cipher block chaining or stream ciphering over multiple packets. For example, encrypted data would advantageously be formed based not only on the contents of the present packet data being encrypted, but also based on some attribute of the connection or session history between the communicating stations. Examples of encryption algorithms and keyed encryption are disclosed in many textbooks, for example "Applied Cryptography - Protocols, Algorithms, and Source Code in C", by Bruce Schneier, published by John Wiley and Sons, New York, New York, copyright 1994.

Thus there is required a new pseudo network adapter providing a virtual private network having a dynamically determined end point to support a user in a mobile computing environment. The new pseudo network adapter should appear to the communications protocol stack of the node as an interface to an actual physical device. The new pseudo network adapter should support guaranteed, in-order delivery of frames over a tunnel to conveniently support cipher block chaining mode or stream cipher encryption over multiple packets.

SUMMARY OF THE INVENTION

A new pseudo network adapter is disclosed providing a virtual private network. The new system includes an interface for capturing packets from a local communications protocol stack for transmission on the virtual private network. The interface appears to the local communications stack as a network adapter device driver for a network adapter.

The invention, in its broad form, includes a pseudo network adapter as recited in claim 1, providing a virtual network and a method therefor as recited in claim 9.

The system as described hereinafter further includes a Dynamic Host Configuration Protocol (DHCP) server emulator, and an Address Resolution Protocol (ARP) server emulator. The new system indicates to the local communications protocol stack that nodes on a remote private network are reachable through a gateway that is in turn reachable through the pseudo network adapter. The new pseudo network adapter includes a transmit path for processing data packets from the local communications protocol stack for transmission through the pseudo network adapter. The transmit path includes an encryption engine for encrypting the data packets and an encapsulation engine for encapsulating the encrypted data packets into tunnel data frames. The pseudo network adapter passes the tunnel data frames back to the local communications protocol stack for transmission to a physical network adapter on a remote server node.

Preferably, as described hereinafter, the pseudo

network adapter includes a digest value in a digest field in each of the tunnel data frames. A keyed hash function is a hash function which takes data and a shared cryptographic key as inputs, and outputs a digital signature referred to as a digest. The value of the digest field is equal to an output of a keyed hash function applied to data consisting of the data packet encapsulated within the tunnel data frame concatenated with a counter value equal to a total number of tunnel data frames previously transmitted to the remote server node. In another aspect of the system, the pseudo network adapter processes an Ethernet header in each one of the captured data packets, including removing the Ethernet header.

The new pseudo network adapter further includes an interface into a transport layer of the local communications protocol stack for capturing received data packets from the remote server node, and a receive path for processing received data packets captured from the transport layer of the local communications protocol stack. The receive path includes a decapsulation engine, and a decryption engine, and passes the decrypted, decapsulated data packets back to the local communications protocol stack for delivery to a user.

Thus there is disclosed a new pseudo network adapter providing a virtual private network having dynamically determined end points to support users in a mobile computing environment. The new pseudo network adapter provides a system for capturing a fully formed frame prior to transmission. The new pseudo network adapter appears to the communications protocol stack of the station as an interface to an actual physical device. The new pseudo network adapter further includes encryption capabilities to conveniently provide secure communications between tunnel end points using stream mode encryption or cipher block chaining over multiple packets.

BRIEF DESCRIPTION OF THE DRAWINGS

A more detailed understanding of the invention may be had from the following description of a preferred embodiment, given by way of example and to be understood in conjunction with the accompanying drawing in which:

- ◆ Fig. 1 is a block diagram showing the Open Systems Interconnection (OSI) reference model;
- ◆ Fig. 2 is a block diagram showing the TCP/IP internet protocol suite;
- ◆ Fig. 3 is a block diagram showing an exemplary embodiment of a tunnel connection across a public network between two tunnel servers;
- ◆ Fig. 4 is a flow chart showing an exemplary embodiment of steps performed to establish a tunnel con-

nection;

- ◆ Fig. 5 is a flow chart showing an exemplary embodiment of steps performed to perform session key management for a tunnel connection; 5
- ◆ Fig. 6 is a block diagram showing an exemplary embodiment of a relay frame;
- ◆ Fig. 7 is a block diagram showing an exemplary embodiment of a connection request frame; 10
- ◆ Fig. 8 is a block diagram showing an exemplary embodiment of a connection response frame; 15
- ◆ Fig. 9 is a block diagram showing an exemplary embodiment of a data frame;
- ◆ Fig. 10 is a block diagram showing an exemplary embodiment of a close connection frame; 20
- ◆ Fig. 11 is a state diagram showing an exemplary embodiment of a state machine forming a tunnel connection in a network node initiating a tunnel connection; 25
- ◆ Fig. 12 is a state diagram showing an exemplary embodiment of a state machine forming a tunnel connection in a server computer; 30
- ◆ Fig. 13 is a state diagram showing an exemplary embodiment of a state machine forming a tunnel connection in a relay node;
- ◆ Fig. 14 is a block diagram showing an exemplary embodiment of a tunnel connection between a client computer (tunnel client) and a server computer (tunnel server); 35
- ◆ Fig. 15 is a block diagram showing an exemplary embodiment of a pseudo network adapter; 40
- ◆ Fig. 16 is a block diagram showing an exemplary embodiment of a pseudo network adapter; 45
- ◆ Fig. 17 is a flow chart showing steps performed by an exemplary embodiment of a pseudo network adapter during packet transmission;
- ◆ Fig. 18 is a flow chart showing steps performed by an exemplary embodiment of a pseudo network adapter during packet receipt; 50
- ◆ Fig. 19 is a data flow diagram showing data flow in an exemplary embodiment of a pseudo network adapter during packet transmission; 55
- ◆ Fig. 20 is a data flow diagram showing data flow in

an exemplary embodiment of a pseudo network adapter during packet receipt;

- ◆ Fig. 21 is a diagram showing the movement of encrypted and unencrypted data in an exemplary embodiment of a system including a pseudo network adapter;
- ◆ Fig. 22 is a diagram showing the movement of encrypted and unencrypted data in an exemplary embodiment of a system including a pseudo network adapter; and
- ◆ Fig. 23 is a flow chart showing steps initialization of an exemplary embodiment of a system including a pseudo network adapter.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Now with reference to Fig. 1 there is described for purposes of explanation, communications based on the Open Systems Interconnection (OSI) reference model. In Fig. 1 there is shown communications 12 between a first protocol stack 10 and a second protocol stack 14. The first protocol stack 10 and second protocol stack 14 are implementations of the seven protocol layers (Application layer, Presentation layer, Session layer, Transport layer, Network layer, Data link layer, and Physical layer) of the OSI reference model. A protocol stack implementation is typically in some combination of software and hardware. Descriptions of the specific services provided by each protocol layer in the OSI reference model are found in many text books, for example "Computer Networks", Second Edition, by Andrew S. Tannenbaum, published by Prentice-Hall, Englewood Cliffs, New Jersey, copyright 1988.

As shown in Fig. 1, data 11 to be transmitted from a sending process 13 to a receiving process 15 is passed down through the protocol stack 10 of the sending process to the physical layer 9 for transmission on the data path 7 to the receiving process 15. As the data 11 is passed down through the protocol stack 10, each protocol layer prepends a header (and possibly also appends a trailer) portion to convey information used by that protocol layer. For example, the data link layer 16 of the sending process wraps the information received from the network layer 17 in a data link header 18 and a data link layer trailer 20 before the message is passed to the physical layer 9 for transmission on the actual transmission path 7.

Fig. 2 shows the TCP/IP protocol stack. Some protocol layers in the TCP/IP protocol stack correspond with layers in the OSI protocol stack shown in Fig. 1. The detailed services and header formats of each layer in the TCP/IP protocol stack are described in many texts, for example "Internetworking with TCP/IP, Vol. 1: Principles, Protocols, and Architecture", Second Edi-

tion, by Douglas E. Comer, published by Prentice-Hall, Englewood Cliffs, New Jersey, copyright 1991. The Transport Control Protocol (TCP) 22 corresponds to the Transport layer in the OSI reference model. The TCP protocol 22 provides a connection-oriented, end to end transport service with guaranteed, in-sequence packet delivery. In this way the TCP protocol 22 provides a reliable, transport layer connection.

The IP protocol 26 corresponds to the Network layer of the OSI reference model. The IP protocol 26 provides no guarantee of packet delivery to the upper layers. The hardware link level and access protocols 32 correspond to the Data link and Physical layers of the OSI reference model.

The Address Resolution Protocol (ARP) 28 is used to map IP layer addresses (referred to as "IP addresses") to addresses used by the hardware link level and access protocols 32 (referred to as "physical addresses" or "MAC addresses"). The ARP protocol layer in each network station typically contains a table of mappings between IP addresses and physical addresses (referred to as the "ARP cache"). When a mapping between an IP address and the corresponding physical address is not known, the ARP protocol 28 issues a broadcast packet (an "ARP request" packet) on the local network. The ARP request indicates an IP address for which a physical address is being requested. The ARP protocols 28 in each station connected to the local network examine the ARP request, and if a station recognizes the IP address indicated by the ARP request, it issues a response (an "ARP response" or "ARP reply" packet) to the requesting station indicating the responder's physical address. The requesting ARP protocol reports the received physical address to the local IP layer which then uses it to send datagrams directly to the responding station. As an alternative to having each station respond only for its own IP address, an ARP server may be used to respond for a set of IP addresses it stores internally, thus potentially eliminating the requirement of a broadcast request. In that case, the ARP request can be sent directly to the ARP server for physical addresses corresponding to any IP address mappings stored within the ARP server.

At system start up, each station on a network must determine an IP address for each of its network interfaces before it can communicate using TCP/IP. For example, a station may need to contact a server to dynamically obtain an IP address for one or more of its network interfaces. The station may use what is referred to as the Dynamic Host Configuration Protocol (DHCP) to issue a request for an IP address to a DHCP server. For example, a DHCP module broadcasts a DHCP request packet at system start up requesting allocation of an IP address for an indicated network interface. Upon receiving the DHCP request packet, the DHCP server allocates an IP address to the requesting station for use with the indicated network interface. The

requesting station then stores the IP address in the response from the server as the IP address to associate with that network interface when communicating using TCP/IP.

Fig. 3 shows an example configuration of network nodes for which the presently disclosed system is applicable. In the example of Fig. 3, the tunnel server A is an initiator of the tunnel connection. As shown in Fig. 3, the term "tunnel relay" node is used to refer to a station which forwards data packets between transport layer connections (for example TCP connections).

For example, in the present system a tunnel relay may be dynamically configured to forward packets between transport layer connection 1 and transport layer connection 2. The tunnel relay replaces the header information of packets received over transport layer connection 1 with header information indicating transport layer connection 2. The tunnel relay can then forward the packet to a firewall, which may be conveniently programmed to pass packets received over transport layer connection 2 into a private network on the other side of the firewall. In the present system, the tunnel relay dynamically forms transport layer connections when a tunnel connection is established. Accordingly the tunnel relay is capable of performing dynamic load balancing or providing redundant service for fault tolerance over one or more tunnel servers at the time the tunnel connection is established.

Fig. 3 shows a Tunnel Server A 46 in a private network N1 48, physically connected with a first Firewall 50. The first Firewall 50 separates the private network N1 48 from a public network 52, for example the Internet. The first Firewall 50 is for example physically connected with a Tunnel Relay B 54, which in turn is virtually connected through the public network 52 with a Tunnel Relay C. The connection between Tunnel Relay B and Tunnel Relay C may for example span multiple intervening forwarding nodes such as routers or gateways through the public network 52.

The Tunnel Relay C is physically connected with a second Firewall 58, which separates the public network 52 from a private network N2 60. The second Firewall 58 is physically connected with a Tunnel Server D 62 on the private network N2 60. During operation of the elements shown in Fig. 3, the Tunnel Server D 62 provides routing of IP packets between the tunnel connection with Tunnel Server A 46 and other stations on the private network N2 60. In this way the Tunnel Server D 62 acts as a router between the tunnel connection and the private network N2 60.

During operation of the elements shown in Fig. 3, the present system establishes a tunnel connection between the private network N1 48 and the private network N2 60. The embodiment of Fig. 3 thus eliminates the need for a dedicated physical cable or line to provide secure communications between the private network 48 and the private network 60. The tunnel connection between Tunnel Server A 46 and Tunnel Server D 62 is

composed of reliable, pair-wise transport layer connections between Tunnel Server A 46 (node "A"), Tunnel Relay B 54 (node "B"), Tunnel Relay C 56 (node "C"), and Tunnel Server D 62 (node "D"). For example, such pair-wise connections may be individual transport layer connections between each node A and node B, node B and node C, and node C and node D. In an alternative embodiment, as will be described below, a tunnel connection may alternatively be formed between a stand-alone PC in a public network and a tunnel server within a private network.

Fig. 4 and Fig. 5 show an example embodiment of steps performed during establishment of the tunnel connection between Tunnel Server A 46 (node "A") and Tunnel Server D 62 (node "D") as shown in Fig. 3. Prior to the steps shown in Fig. 4, node A selects a tunnel path to reach node D. The tunnel path includes the tunnel end points and any intervening tunnel relays. The tunnel path is for example predetermined by a system administrator for node A. Each tunnel relay along the tunnel path is capable of finding a next node in the tunnel path, for example based on a provided next node name (or "next node arc"), using a predetermined naming convention and service, for example the Domain Name System (DNS) of the TCP/IP protocol suite.

During the steps shown in Fig. 4, each of the nodes A, B and C perform the following steps:

- resolve the node name of the next node in the tunnel path, for example as found in a tunnel relay frame;
- establish a reliable transport layer (TCP) connection to the next node in the tunnel path;
- forward the tunnel relay frame down the newly formed reliable transport layer connection to the next node in the tunnel path.

As shown for example in Fig. 4, at step 70 node A establishes a reliable transport layer connection with node B. At step 72 node A identifies the next downstream node to node B by sending node B a tunnel relay frame over the reliable transport layer connection between node A and node B. The tunnel relay frame contains a string buffer describing all the nodes along the tunnel path (see below description of an example tunnel relay frame format). At step 74, responsive to the tunnel relay frame from node A, node B searches the string buffer in the relay frame to determine if the string buffer includes node B's node name. If node B finds its node name in the string buffer, it looks at the next node name in the string buffer to find the node name of the next node in the tunnel path.

Node B establishes a reliable transport layer connection with the next node in the tunnel path, for example node C. Node B further forms an association between the reliable transport layer connection between

Node A and Node B, over which the relay frame was received, and the newly formed reliable transport layer connection between Node B and Node C, and as a result forwards subsequent packets received over the reliable transport layer connection with Node A onto the reliable transport layer connection with Node C, and vice versa. At step 76 node B forwards the tunnel relay frame on the newly formed reliable transport layer connection to node C.

At step 78, responsive to the relay frame forwarded from node B, node C determines that the next node in the tunnel path is the last node in the tunnel path, and accordingly is a tunnel server. Node C may actively determine whether alternative tunnel servers are available to form the tunnel connection. Node C may select one of the alternative available tunnel servers to form the tunnel connection in order to provide load balancing or fault tolerance. As a result node C may form a transport layer connections with one of several available tunnel servers, for example a tunnel server that is relatively underutilized at the time the tunnel connection is established. In the example embodiment, node C establishes a reliable transport layer connection with the next node along the tunnel path, in this case node D.

Node C further forms an association between the reliable transport layer connection between Node B and Node C, over which the relay frame was received, and the newly formed reliable transport layer connection between Node C and Node D, and as a result forwards subsequent packets received over the reliable transport layer connection with Node B to the reliable transport layer connection with Node D, and vice versa. At step 80 node C forwards the relay frame to node D on the newly formed reliable transport layer connection.

Fig. 5 shows an example of tunnel end point authentication and sharing of key exchange material provided by the present system. The present system supports passing authentication data and key exchange material through the reliable transport layer connections previously established on the tunnel path. The following are provided by use of a key exchange/authentication REQUEST frame and a key exchange/authentication RESPONSE frame:

- a) mutual authentication of both endpoints of the tunnel connection;
- b) establishment of shared session encryption keys and key lifetimes for encrypting/authenticating subsequent data sent through the tunnel connection;
- d) agreement on a shared set of cryptographic transforms to be applied to subsequent data; and
- e) exchange of any other connection-specific data between the tunnel endpoints, for example strength and type of cipher to be used, any compression of the data to be used, etc. This data can also be used

by clients of this protocol to qualify the nature of the authenticated connection.

At step 90 a key exchange/authentication request frame is forwarded over the reliable transport layer connections formed along the tunnel path from node A to node D. At step 92, a key exchange/authentication response frame is forwarded from node D back to node A through the reliable transport layer connections. The attributes exchanged using the steps shown in Fig. 5 may be used for the lifetime of the tunnel connection. In an alternative embodiment the steps shown in Fig. 5 are repeated as needed for the tunnel end points to exchange sufficient key exchange material to agree upon a set of session parameters for use during the tunnel connection such as cryptographic keys, key durations, and choice of encryption/decryption algorithms.

Further in the disclosed system, the names used for authentication and access control with regard to node A and node D need not be the network layer address or physical address of the nodes. For example, in an alternative embodiment where the initiating node sending the tunnel relay frame is a stand-alone PC located within a public network, the user's name may be used for authentication and/or access control purposes. This provides a significant improvement over existing systems which base authorization on predetermined IP addresses.

Fig. 6 shows the format of an example embodiment of a tunnel relay frame. The tunnel frame formats shown in Figs. 6, 7, 8 and 9 are encapsulated within the data portion of a transport layer (TCP) frame when transmitted. Alternatively, another equivalent, connection-oriented transport layer protocol having guaranteed, in-sequence frame delivery may be used. The example TCP frame format, including TCP header fields, is conventional and not shown.

The field 100 contains a length of the frame. The field 102 contains a type of the frame, for example a type of RELAY. The field 104 contains a tunnel protocol version number. The field 106 contains an index into a string buffer field 112 at which a name of the originating node is located, for example a DNS host name of the node initially issuing the relay frame (node A in Fig. 3). The fields following the origin index field 106 contain indexes into the string buffer 112 at which names of nodes along the tunnel path are located. For example each index may be the offset of a DNS host name within the string buffer 112. In this way the field 108 contains the index of the name of the first node in the tunnel path, for example node B (Fig. 3). The field 110 contains the index of the name of the second node in the tunnel path, etc. The field 112 contains a string of node names of nodes in the tunnel path.

During operation of the present system, the initiating node, for example node A as shown in Fig. 3, transmits a tunnel relay frame such as the tunnel relay frame shown in Fig. 6. Node A sends the tunnel relay frame to

the first station along the tunnel path, for example node B (Fig. 3), over a previously established reliable transport layer connection. Node B searches the string buffer in the tunnel relay frame to find its node name, for example its DNS host name. Node B finds its node name in the string buffer indexed by path index 0, and then uses the contents of path index 1 110 to determine the location within the string buffer 112 of the node name of the next node along the tunnel path. Node B uses this node name to establish a reliable transport layer connection with the next node along the tunnel path. Node B then forwards the relay frame to the next node. This process continues until the end node of the tunnel route, for example tunnel server D 62 (Fig. 3) is reached.

Fig. 7 shows the format of an example embodiment of a key exchange/key authentication request frame. The field 120 contains a length of the frame. The field 122 contains a type of the frame, for example a type of REQUEST indicating a key exchange/key authentication request frame. The field 124 contains a tunnel protocol version number. The field 126 contains an offset of the name of the entity initiating the tunnel connection, for example the name of a user on the node originally issuing the request frame. This name and key exchange material in the request frame are used by the receiving tunnel end point to authenticate the key exchange/authentication REQUEST. The name of the entity initiating the tunnel connection is also used to authorize any subsequent tunnel connection, based on predetermined security policies of the system. The field 128 contains an offset into the frame of the node name of the destination node, for example the end node of the tunnel shown as node D 62 in Fig. 3.

The field 130 contains an offset into the frame at which key exchange data as is stored, for example within the string buffer field 138. The key exchange data for example includes key exchange material used to determine a shared set of encryption parameters for the life of the tunnel connection such as cryptographic keys and any validity times associated with those keys. The key exchange data, as well as the field 132, further include information regarding any shared set of cryptographic transforms to be used and any other connection-specific parameters, such as strength and type of cipher to be used, type of compression of the data to be used, etc. The field 134 contains flags, for example indicating further information about the frame. The field 136 contains client data used in the tunnel end points to configure the local routing tables so that packets for nodes reachable through the virtual private network are sent through the pseudo network adapters. In an example embodiment, the string buffer 138 is encrypted using a public encryption key of the receiving tunnel end point.

During operation of the present system, one of the end nodes of the tunnel sends a key exchange/authentication REQUEST frame as shown in Fig. 7 to the other end node of the tunnel in order to perform key exchange and authentication as described in step 90 of Fig. 5.

Fig. 8 shows the format of an example embodiment of a key exchange/key authentication response frame, referred to as a connection RESPONSE frame. The field 150 contains a length of the frame. The field 152 contains a type of the frame, for example a type of connection RESPONSE indicating a key exchange/key authentication request frame. The field 154 contains a tunnel protocol version number.

The field 156 contains an offset into the frame at which key exchange data as is stored, for example within the string buffer field 163. The key exchange data for example includes key exchange material to be used for encryption/decryption over the life of the tunnel connection and any validity times associated with that key exchange material. The key exchange data, as well as the field 158, further includes information regarding any shared set of cryptographic transforms to be applied to subsequent data and any other connection-specific parameters, such as strength and type of cipher to be used, any compression of the data to be used, etc. The field 160 contains flags, for example indicating other information about the frame. The client data field 162 contains data used by the pseudo network adapters in the tunnel end points to configure the local routing tables so that packets for nodes in the virtual private network are sent through the pseudo network adapters. The string buffer includes key exchange material. The string buffer is for example encrypted using a public encryption key of the receiving tunnel end point, in this case the initiator of the tunnel connection.

During operation of the present system, one of the end nodes of the tunnel sends a key exchange/authentication RESPONSE frame as shown in Fig. 7 to the other end node of the tunnel in order to perform key exchange and authentication as described in step 92 of Fig. 5.

Fig. 9 shows the format of an example embodiment of an tunnel data frame used to communicate through a tunnel connection. Fig. 9 shows how an IP datagram may be encapsulated within a tunnel frame by the present system for secure communications through a virtual private network. The field 170 contains a length of the frame. The field 172 contains a type of the frame, for example a type of DATA indicating a tunnel data frame. The field 174 contains a tunnel protocol version number.

The fields 176, 178 and 182 contain information regarding the encapsulated datagram. The field 180 contains flags indicating information regarding the frame. The field 184 contains a value indicating the length of the optional padding 189 at the end of the frame. The frame format allows for optional padding in the event that the amount of data in the frame needs to be padded to an even block boundary for the purpose of being encrypted using a block cipher. The field 186 contains a value indicating the length of the digest field 187.

The data frame format includes a digital signature generated by the transmitting tunnel end point referred

to as a "digest". The value of the digest ensures data integrity, for example by detecting invalid frames and replays of previously transmitted valid frames. The digest is the output of a conventional keyed cryptographic hash function applied to both the encapsulated datagram 190 and a monotonically increasing sequence number. The resulting hash output is passed as the value of the digest field 187. The sequence number is not included in the data frame. In the example embodiment, the sequence number is a counter maintained by the transmitter (for example node A in Fig. 3) of all data frames sent to the receiving node (for example node D in Fig. 3) since establishment of the tunnel connection.

In order to determine if the data frame is invalid or a duplicate, the receiving node decrypts the encapsulated datagram 190, and applies the keyed cryptographic hash function (agreed to by the tunnel end nodes during the steps shown in Fig. 5) to both the decrypted encapsulated datagram and the value of a counter indicating the number of data frames received from the transmitter since establishment of the tunnel connection. For example the keyed hash function is applied to the datagram concatenated to the counter value. If the resulting hash output matches the value of the digest field 187, then the encapsulated datagram 190 was received correctly and is not a duplicate. If the hash output does not match the value of the digest field 187, then the integrity check fails, and the tunnel connection is closed. The field 188 contains an encrypted network layer datagram, for example an encrypted IP datagram.

The encapsulated datagram may be encrypted using various encryption techniques. An example embodiment of the present system advantageously encrypts the datagram 190 using either a stream cipher or cipher block chaining encryption over all data transmitted during the life of the tunnel connection. This is enabled by the reliable nature of the transport layer connections within the tunnel connection. The specific type of encryption and any connection specific symmetric encryption keys used is determined using the steps shown in Fig. 5. The fields in the tunnel data frame other than the encapsulated datagram 188 are referred to as the tunnel data frame header fields.

Fig. 10 is a block diagram showing an example embodiment of a "close connection" frame. The field 190 contains the length of the frame. The field 191 contains a frame type, for example having a value equal to CLOSE. Field 192 contains a value equal to the current protocol version number of the tunnel protocol. The field 193 contains a status code indicating the reason the tunnel connection is being closed.

During operation of the present system, when end point of a tunnel connection determines that the tunnel connection should be closed, a close connection frame as shown in Fig. 10 is transmitted to the other end point of the tunnel connection. When a close connection close frame is received, the receiver closes the tunnel

connection and no further data will be transmitted or received through the tunnel connection.

Fig. 11 is a state diagram showing an example embodiment of forming a tunnel connection in a node initiating a tunnel connection. In Fig. 11, Fig. 12, and Fig. 13, states are indicated by ovals and actions or events are indicated by rectangles. For example the tunnel server node A as shown in Fig. 3 may act as a tunnel connection initiator when establishing a tunnel connection with the tunnel server node D. Similarly the client system 247 in Fig. 14 may act as a tunnel connection initiator when establishing a tunnel connection with the tunnel server. The tunnel initiator begins in an idle state 194. Responsive to an input from a user indicating that a tunnel connection should be established, the tunnel initiator transitions from the idle state 194 to a TCP Open state 195. In the TCP Open state 195, the tunnel initiator establishes a reliable transport layer connection with a first node along the tunnel path. For example, the tunnel initiator opens a socket interface associated with a TCP connection to the first node along the tunnel path. In Fig. 3 node A opens a socket interface associated with a TCP connection with node B.

Following establishment of the reliable transport layer connection in the TCP Open state 195, the tunnel initiator enters a Send Relay state 197. In the Send Relay state 197, the tunnel initiator transmits a relay frame at 198 over the reliable transport layer connection. Following transmission of the relay frame, the tunnel initiator enters the connect state 199. If during transmission of the relay frame there is a transmission error, the tunnel initiator enters the Network Error state 215 followed by the Dying state 208. In the Dying state 208, the tunnel initiator disconnects the reliable transport layer connection formed in the TCP Open state 195, for example by disconnecting a TCP connection with Node B. Following the disconnection at 209, the tunnel initiator enters the Dead state 210. The tunnel initiator subsequently transitions back to the Idle state 194 at a point in time predetermined by system security configuration parameters.

In the Connect state 199, the tunnel initiator sends a key exchange/authentication REQUEST frame at 200 to the tunnel server. Following transmission of the key exchange/authentication REQUEST frame 200, the tunnel initiator enters the Response Wait state 201. The tunnel initiator remains in the Response Wait state 201 until it receives a key exchange/authentication RESPONSE frame 202 from the tunnel server. After the key exchange/authentication RESPONSE frame is received at 202, the tunnel initiator enters the Authorized state 203, in which it may send or receive tunnel data frames. Upon receipt of a CLOSE connection frame at 216 in the Authorized state 203, the tunnel initiator transitions to the Dying state 208.

Upon expiration of a session encryption key at 211, the tunnel initiator enters the Reconnect state 212, and sends a CLOSE connection frame at 213 and discon-

nects the TCP connection with the first node along the tunnel path at 214. Subsequently the tunnel initiator enters the TCP Open state 195.

If during the authorized state 203, a local user issues an End Session command at 204, or there is a detection of an authentication or cryptography error in a received data frame at 205, the tunnel initiator enters the Close state 206. During the Close state 206 the tunnel initiator sends a CLOSE connection frame at 207 to the tunnel server. The tunnel initiator then enters the Dying state at 208.

Figure 12 is a state diagram showing the states within an example embodiment of a tunnel server, for example node D in Fig. 3 or tunnel server 253 in Fig. 14. The tunnel server begins in an Accept Wait state 217. In the Accept Wait state 217, the tunnel server receives a request for a reliable transport layer connection, for example a TCP connection request 218 from the last node in the tunnel path prior to the tunnel server, for example Node C in Fig. 3. In response to a TCP connection request 218 the tunnel server accepts the request and establishes a socket interface associated with the resulting TCP connection with Node C.

Upon establishment of the TCP connection with the last node in the tunnel path prior to the tunnel server, the tunnel server enters the Receive Relay state 219. In the Receive Relay state 219, the tunnel server waits to receive a relay frame at 220, at which time the tunnel server enters the Connect Wait state 221. If there is some sort of network error 234 during receipt of the relay frame at 219, the tunnel server enters the Dying state 230. During the Dying state 230 the tunnel server disconnects at 231 the transport layer connection with the last node in the tunnel path prior to the tunnel server. After disconnecting the connection, the tunnel server enters the Dead state 232.

In the Connect Wait state 221, the tunnel server waits for receipt of a key exchange/authentication REQUEST frame at 222. Following receipt of the key exchange/authentication REQUEST frame at 222, the tunnel server determines whether the requested tunnel connection is authorized at step 223. The determination of whether the tunnel connection is authorized is based on a name of the tunnel initiator, and the key exchange material within the key exchange/authentication REQUEST frame.

If the requested tunnel connection is authorized the tunnel server sends a key exchange/authentication RESPONSE frame at 224 back to the tunnel initiator. If the requested tunnel connection is not authorized, the tunnel server enters the Close state 228, in which it sends a close connection frame at 229 to the tunnel client. Following transmission of the CLOSE connection frame at 229, the tunnel server enters the Dying state 230.

If the requested tunnel connection is determined to be authorized at step 223, the tunnel server enters the Authorized state 225. In the Authorized state, the tunnel

server transmits and receives tunnel data frames between itself and the tunnel initiator. If during the Authorized state 225, the tunnel server receives a CLOSE connection frame at 233, the tunnel server transitions to the Dying state 230. If during the authorized state 225, the tunnel server receives an end session command from a user at 226, then the tunnel server transitions to the Close state 228, and transmits a close connection frame at 229 to the tunnel initiator. If the tunnel server in the Authorized state 225 detects an integrity failure in a received packet, the tunnel server transitions to the Close state 228. In the close state 228 the tunnel server sends a CLOSE connection frame at 229 and subsequently enters the Dying state 230.

Fig. 13 is a state diagram showing an example embodiment of a state machine within a tunnel relay node. The tunnel relay node begins in an Accept Wait state 235. When a request is received to form a reliable transport layer connection at 236, a reliable transport layer connection is accepted with the requesting node. For example, a TCP connection is accepted between the relay node and the preceding node in the tunnel path.

The relay node then transitions to the Receive Relay state 237. During the Receive Relay state 237, the relay node receives a relay frame at 238. Following receipt of the relay frame at 238, the relay node determines what forwarding address should be used to forward frames received from the TCP connection established responsive to the TCP connect event 236. If the next node in the tunnel path is a tunnel server, the forwarding address may be selected at 239 so as to choose an underutilized tunnel server from a group of available tunnel servers or to choose an operational server where others are not operational.

Following determination of the forwarding address or addresses in step 239, the relay node enters the Forward Connect state 240. In the Forward Connect state 240, the relay node establishes a reliable transport layer connection with the node or nodes indicated by the forwarding address or addresses determined in step 239.

Following establishment of the new connection at event 241, the tunnel relay enters the Forward state 242. During the Forward state 242, the relay node forwards all frames between the connection established at 236 and those connections established at 241. Upon detection of a network error or receipt of a frame indicating a closure of the tunnel connection at 243, the tunnel relay enters the Dying state 244. Following the Dying state 244, the relay node disconnects any connections established at event 241. The relay node then enters the Dead state 246.

Fig. 14 shows an example embodiment of a virtual private network 249 formed by a pseudo network adapter 248 and a tunnel connection between a tunnel client 247 and a tunnel server 253 across a public network 251. The tunnel server 253 and tunnel client 247 are for example network stations including a CPU or

microprocessor, memory, and various I/O devices. The tunnel server 253 is shown physically connected to a private LAN 256 including a Network Node 1 257 and a Network Node 2 258, through a physical network adapter 254. The tunnel server 253 is further shown physically connected with a firewall 252 which separates the private LAN 256 from the public network 251. The firewall 252 is physically connected with the public network 251. The tunnel server 253 is further shown including a pseudo network adapter 255. The client system 247 is shown including a physical network adapter 250 physically connected to the public network 251.

During operation of the elements shown in Fig. 14, nodes within the virtual private network 249 appear to the tunnel client 247 as if they were physically connected to the client system through the pseudo network adapter 248. Data transmissions between the tunnel client and any nodes that appear to be within the virtual private network are passed through the pseudo network adapter 248. Data transmissions between the tunnel client 247 and the tunnel server 253 are physically accomplished using a tunnel connection between the tunnel client 247 and the tunnel server 253.

Fig. 15 shows elements in an example embodiment of a pseudo network adapter such as the pseudo network adapter 248 in Fig. 14. In an example embodiment the elements shown in Fig. 15 are implemented as software executing on the tunnel client 247 as shown in Fig. 14. In Fig. 15 there is shown a pseudo network adapter 259 including a virtual adapter driver interface 263, an encapsulation engine 264, an encryption engine 265, a decapsulation engine 268, and a decryption engine 266. Further shown in the pseudo network adapter 259 are an ARP server emulator 270 and a Dynamic Host Configuration Protocol (DHCP) server emulator.

The pseudo network adapter 259 is shown interfaced to a TCP/IP protocol stack 260, through the virtual adapter driver interface 260. The TCP/IP protocol stack 260 is shown interfaced to other services in an operating system 261, as well as a physical network adapter's driver 262. The physical network adapter's driver 262 is for example a device driver which controls the operation of a physical network adapter such as physical network adapter 250 as shown in Fig. 14.

During operation of the elements shown in Fig. 15, the pseudo network adapter 259 registers with the network layer in the TCP/IP stack 260 that it is able to reach the IP addresses of nodes within the virtual private network 249 as shown in Fig. 14. For example, the pseudo network adapter on the client system registers that it can reach the pseudo network adapter on the server. Subsequently, a message from the tunnel client addressed to a node reachable through the virtual private network will be passed by the TCP/IP stack to the pseudo network adapter 259. The pseudo network adapter 259 then encrypts the message, and encapsulates the message into a tunnel data frame. The pseudo network adapter 259 then passes the tunnel data frame

back to the TCP/IP protocol stack 260 to be sent through to the physical network adapter in the tunnel server. The tunnel server passes the received data frame to the pseudo network adapter in the server, which de-encapsulates and decrypts the message.

Fig. 16 shows a more detailed example embodiment of a pseudo network adapter 280. The pseudo network adapter 280 includes a virtual network adapter driver interface 288. The transmit path 290 includes an encryption engine 292, and an encapsulation engine 294. The encapsulation engine 294 is interfaced with a TCP/IP transmit interface 312 within a TCP/IP protocol stack, for example a socket interface associated with the first relay node in the tunnel path, or with the remote tunnel end point if the tunnel path includes no relays.

In the example embodiment of Fig. 16, the pseudo network adapter 280 appears to the TCP/IP protocol stack 282 as an Ethernet adapter. Accordingly, ethernet packets 286 for a destination addresses understood by the TCP/IP protocol stack to be reachable through the virtual private network are passed from the TCP/IP protocol stack 282 to the virtual network adapter interface 288 and through the transmit path 290. Similarly, ethernet packets 284 received through the pseudo network adapter 280 are passed from the receive path 296 to the virtual network adapter interface 288 and on to the TCP/IP protocol stack 282.

Further shown in the pseudo network adapter 280 of Fig. 16 is a receive path 296 having a decryption engine 298 interfaced to the virtual network adapter interface 288 and a decapsulation engine 300. The decapsulation engine 300 in turn is interfaced to a TCP/IP receive function 314 in the TCP/IP protocol stack 282, for example a socket interface associated with the first relay in the tunnel path, or with the remote tunnel end point if the tunnel path includes no relays. The pseudo network adapter 280 further includes an ARP server emulator 304 and a DHCP server emulator 306. ARP and DHCP request packets 302 are passed to the ARP server emulator 304 and DHCP server emulator 306 respectively. When a received packet is passed from the receive path 296 to the TCP/IP stack 282, a receive event must be indicated to the TCP/IP stack 282, for example through an interface such the Network Device Interface Specification (NDIS), defined by Microsoft™ Corporation.

Also in Fig. 16 is shown is an operating system 310 coupled with the TCP/IP protocol stack 282. The TCP/IP protocol stack 282 is generally considered to be a component part of the operating system. The operating system 310 in Fig. 16 is accordingly the remaining operating system functions and procedures outside the TCP/IP protocol stack 282. A physical network adapter 308 is further shown operated by the TCP/IP protocol stack 282.

During operation of the elements shown in Fig. 16, a user passes data for transmission to the TCP/IP protocol stack 282, and indicates the IP address of the

node to which the message is to be transmitted, for example through a socket interface to the TCP layer. The TCP/IP protocol stack 282 then determines whether the destination node is reachable through the virtual private network. If the message is for a node that is reachable through the virtual private network, the TCP/IP protocol stack 282 an ethernet packet 286 corresponding to the message to the pseudo network adapter 280. The pseudo network adapter 280 then passes the ethernet packet 286 through the transmit path, in which the ethernet packet is encrypted and encapsulated into a tunnel data frame. The tunnel data frame is passed back into the TCP/IP protocol stack 282 through the TCP/IP transmit function 312 to be transmitted to the tunnel server through the tunnel connection. In an example embodiment, a digest value is calculated for the tunnel data frame before encryption within the transmit path within the pseudo network adapter.

Further during operation of the elements shown in Fig. 16, when the TCP/IP protocol stack 282 receives a packet from the remote endpoint of the TCP/IP tunnel connection, for example the tunnel server, the packet is passed to the pseudo network adapter 280 responsive to a TCP receive event. The pseudo network adapter 280 then decapsulates the packet by removing the tunnel header. The pseudo network adapter further decrypts the decapsulated data and passes it back to the TCP/IP protocol stack 282. The data passed from the pseudo network adapter 280 appears to the TCP/IP protocol stack 282 as an ethernet packet received from an actual physical device, and is the data it contains is passed on to the appropriate user by the TCP/IP protocol stack 282 based on information in the ethernet packet header provided by the pseudo network adapter.

Fig. 17 is a flow chart showing steps performed by an example embodiment of a pseudo network adapter during packet transmission, such as in the transmit path 290 of Fig. 14. The TCP/IP protocol stack determines that the destination node of a packet to be transmitted is reachable through the virtual LAN based on the destination IP address of the packet and a network layer routing table. At step 320 the packet is passed to the pseudo network adapter from the TCP/IP protocol stack. As a result, a send routine in the pseudo adapter is triggered for example in the virtual network adapter interface 288 of Fig. 16.

At step 322 the pseudo network adapter send routine processes the Ethernet header of the packet provided by the TCP/IP stack, and removes it. At step 324, the send routine determines whether the packet is an ARP request packet. If the packet is an ARP request packet for an IP address of a node on the virtual LAN, such as the pseudo network adapter of the tunnel server, then step 324 is followed by step 326. Otherwise, step 324 is followed by step 330.

At step 326, the ARP server emulator in the pseudo network adapter generates an ARP reply packet. For example, if the ARP request were for a physical address

corresponding to the IP address of the pseudo network adapter on the tunnel server, the ARP reply would indicate a predetermined, reserved physical address to be associated with that IP address. At step 328 the pseudo network adapter passes the ARP response to the virtual network adapter interface. The virtual network adapter interface then indicates a received packet to the TCP/IP protocol stack, for example using an NDIS interface. The TCP/IP protocol stack then processes the ARP response as if it had been received over an actual physical network.

At step 330 the send routine determines whether the packet is a DHCP request packet requesting an IP address for the pseudo network adapter. If so, then step 330 is followed by step 332. Otherwise, step 330 is followed by step 334.

At step 334, the DHCP server emulator in the pseudo network adapter generates a DHCP response. The format of DHCP is generally described in the DHCP RFC. At step 328 the pseudo network adapter passes the DHCP response to the virtual network adapter interface, for example indicating an IP address received from the tunnel server in the client data field of the key exchange/authentication RESPONSE frame. The virtual network adapter interface then indicates a received packet to the TCP/IP protocol stack. The TCP/IP protocol stack then processes the DHCP response as if it had been received over an actual physical network.

At step 334 the pseudo network adapter encrypts the message using an encryption engine such that only the receiver is capable of decrypting and reading the message. At step 336 the pseudo network adapter encapsulates the encrypted message into a tunnel data frame. At step 338 the pseudo network adapter transmits the tunnel data frame through the tunnel connection using the TCP/IP protocol stack.

Fig. 18 is a flow chart showing steps performed by an example embodiment of a pseudo network adapter during packet receipt, such as in the receive path 296 of Fig. 14.

At step 350, the pseudo network adapter is notified that a packet has been received over the tunnel connection. At step 352 the pseudo network adapter decapsulates the received message by removing the header fields of the tunnel data frame. At step 354 the pseudo network adapter decrypts the decapsulated datagram from the tunnel data frame. At step 356, in an example embodiment, the pseudo network adapter forms an Ethernet packet from the decapsulated message. At step 358 the pseudo network adapter indicates that an Ethernet packet has been received to the TCP/IP protocol stack through the virtual network adapter interface. This causes the TCP/IP protocol stack to behave as if it had received an Ethernet packet from an actual Ethernet adapter.

Fig. 19 shows the data flow within the transmit path in an example embodiment of a pseudo network adapter. At step 1 370, an application submits data to be

transmitted to the TCP protocol layer 372 within the TCP/IP protocol stack. The application uses a conventional socket interface to the TCP protocol layer 372 to pass the data, and indicates the destination IP address the data is to be transmitted to. The TCP protocol layer 372 then passes the data to the IP protocol layer 374 within the TCP/IP protocol stack. At step 2 376, the TCP/IP protocol stack refers to the routing table 378 to determine which network interface should be used to reach the destination IP address.

Because in the example the destination IP address is of a node reachable through the virtual private network, the IP layer 374 determines from the routing table 378 that the destination IP address is reachable through pseudo network adapter. Accordingly at step 3 380 the TCP/IP protocol stack passes a packet containing the data to the pseudo network adapter 382.

At step 4 384, the pseudo network adapter 382 encrypts the data packets and encapsulates them into tunnel data frames.

The pseudo network adapter 382 then passes the tunnel data frames packets back to the TCP protocol layer 372 within the TCP/IP protocol stack through a conventional socket interface to the tunnel connection with the first node in the tunnel path.

The TCP protocol layer 372 then forms a TCP layer packet for each tunnel data frame, having the tunnel data frame as its data. The TCP frames are passed to the IP layer 374. At step 5 386 the routing table 378 is again searched, and this time the destination IP address is the IP address associated with the physical network adapter on the tunnel server, and accordingly is determined to be reachable over the physical network adapter 390. Accordingly at step 6 388 the device driver 390 for the physical network adapter is called to pass the packets to the physical network adapter. At step 7 392 the physical network adapter transmits the data onto the physical network 394.

Fig. 20 is a data flow diagram showing data flow in an example embodiment of packet receipt involving a pseudo network adapter. At step 1 410 data arrives over the physical network 412 and is received by the physical network adapter and passed to the physical network driver 414. The physical network driver 414 passes the data at step 2 418 through the IP layer 420 and TCP layer 422 to the pseudo network adapter 426 at step 3 424, for example through a conventional socket interface. At step 4 428 the pseudo network adapter 426 decrypts and decapsulates the received data and passes it back to the IP layer of the TCP/IP protocol stack, for example through the TDI (Transport Layer Dependent Interface API) of the TCP/IP stack. The data is then passed through the TCP/IP protocol stack and to the user associated with the destination IP address in the decapsulated datagrams at step 5 430.

Fig. 21 shows data flow in an example embodiment of packet transmission involving a pseudo network adapter. Fig. 21 shows an example embodiment for use

on a Microsoft™ Windows 95™ PC platform. In Fig. 21 a user application 450 passes unencrypted data to an interface into the TCP layer of the TCP/IP protocol, for example the WinSock API 452. The user indicates a destination IP address associated with a node reachable through a virtual private network accessible through the pseudo network adapter.

The TCP layer 454 passes the data to the IP layer 456, which in turn passes the data to the Network Device Interface Specification Media Access Control (NDIS MAC) interface 458. The pseudo network adapter 459 has previously registered with the routing layer (IP) that it is able to reach a gateway address associated with the destination IP address for the user data. Accordingly the IP layer uses the NDIS MAC layer interface to invoke the virtual device driver interface 460 to the pseudo network adapter 459. The pseudo network adapter 459 includes a virtual device driver interface 460, an ARP server emulator 462, and a DHCP server emulator 464.

In the example embodiment of Fig. 19, the pseudo network adapter 459 passes the data to a tunnel application program 466. The tunnel application program 466 encrypts the IP packet received from the IP layer and encapsulates it into a tunnel data frame. The tunnel application then passes the tunnel data frame including the encrypted data to the WinSock interface 452, indicating a destination IP address of the remote tunnel end point. The tunnel data frame is then passed through the TCP layer 454, IP layer 456, NDIS MAC layer interface 458, and physical layer 468, and transmitted on the network 470. Since the resulting packets do not contain a destination IP address which the pseudo network adapter has registered to convey, these packets will not be diverted to the pseudo network adapter.

Fig. 22 is a data flow diagram showing data flow in an example embodiment of packet transmission involving a pseudo network adapter. The embodiment shown in Fig. 22 is for use on a UNIX platform. In Fig. 20 a user application 472 passes unencrypted data to a socket interface to the TCP/IP protocol stack in the UNIX socket layer 474, indicating a destination IP address of a node reachable through the virtual private network.

The UNIX socket layer 474 passes the data through the TCP layer 476 and the IP layer 478. The pseudo network adapter 480 has previously registered with the routing layer (IP) that it is able to reach a gateway associated with the destination IP address for the user data. Accordingly the IP layer 478 invokes the virtual device driver interface 482 to the pseudo network adapter 480. The IP layer 478 passes the data to the pseudo network adapter 480. The pseudo network adapter 480 includes a virtual device driver interface 482, and a DHCP server emulator 484.

In the example embodiment of Fig. 22, the pseudo network adapter 480 passes IP datagrams to be transmitted to a UNIX Daemon 486 associated with the tunnel connection. The UNIX Daemon 486 encrypts the IP

packet(s) received from the IP layer 478 and encapsulates them into tunnel data frames. The UNIX Daemon 486 then passes the tunnel data frames to the UNIX socket layer 474, through a socket associated with the tunnel connection. The tunnel data frames are then processed by the TCP layer 476, IP layer 478, data link layer 488, and physical layer 490 to be transmitted on the network 492. Since the resulting packets are not addressed to an IP address which the pseudo network adapter 480 has registered to convey, the packets will not be diverted to the pseudo network adapter 480.

Fig. 23 is a flow chart showing steps to initialize a example embodiment of a virtual private network. The steps shown in Fig. 23 are performed for example in the tunnel client 247 as shown in Fig. 14. At step 500 a tunnel application program executing in the tunnel client sends a tunnel relay frame to the tunnel server. At step 502 the tunnel application program sends a tunnel key exchange/authentication REQUEST frame to the tunnel server. The tunnel application in the tunnel server ignores the contents of the client data field in the tunnel key exchange/authentication REQUEST frame. The tunnel application in the tunnel server fills in the client data field in the tunnel key exchange/authentication RESPONSE frame with Dynamic Host Configuration Protocol (DHCP) information, for example including the following information in standard DHCP format:

- 1) IP Address for tunnel client Pseudo Network Adapter
- 2) IP Address for tunnel server Pseudo Network Adapter
- 3) Routes to nodes on the private network physically connected to the tunnel server which are to be reachable over the tunnel connection.

At step 504 the tunnel application receives a tunnel key exchange/authentication RESPONSE frame from the tunnel server. The client data field 508 in the tunnel connection response is made available to the pseudo network adapter in the tunnel client. The tunnel application in the tunnel client tells the TCP/IP stack that the pseudo network adapter in the tunnel client is active. The pseudo network adapter in the tunnel client is active and ready to be initialized at step 510.

The tunnel client system is configured such that it must obtain an IP address for the tunnel client pseudo network adapter dynamically. Therefore the TCP/IP stack in the tunnel client broadcasts a DHCP request packet through the pseudo network adapter. Accordingly, at step 512 the pseudo network adapter in the client receives a conventional DHCP request packet from the TCP/IP stack requesting a dynamically allocated IP address to associate with the pseudo network adapter. The pseudo network adapter passes the DHCP request packet to the DHCP server emulator within the pseudo network adapter, which forms a DHCP response based on the client data 508 received from the tunnel applica-

tion. The DHCP response includes the IP address for the client pseudo adapter provided by the tunnel server in the client data. At step 514 the pseudo network adapter passes the DHCP response to the TCP/IP stack.

At step 520, the tunnel application modifies the routing tables within the tunnel client TCP/IP stack to indicate that the routes to the nodes attached to the private network to which the tunnel server is attached all are reachable only through the pseudo network adapter in the tunnel server. The IP address of the pseudo network adapter in the tunnel server provided in the client data is in this way specified as a gateway to the nodes on the private network to which the tunnel server is attached. In this way those remote nodes are viewed by the TCP/IP stack as being reachable via the virtual private network through the client pseudo network adapter.

At step 516 the pseudo network adapter in the tunnel client receives an ARP request for a physical address associated with the IP address of the pseudo network adapter in the tunnel server. The pseudo network adapter passes the ARP request to the ARP server emulator, which forms an ARP reply indicating a reserved physical address to be associated with the IP address of the pseudo network adapter in the tunnel server. At step 518 the pseudo network adapter passes the ARP response to the TCP/IP stack in the tunnel client. In response to the ARP response, the TCP/IP stack determines that packets addressed to any node on the virtual private network must be initially transmitted through the pseudo network adapter.

In an example embodiment the present system reserves two physical addresses to be associated with the pseudo network adapter in the client and the pseudo network adapter in the server respectively. These reserved physical addresses are used in responses to ARP requests passed through the pseudo network adapter for physical addresses corresponding to the IP addresses for the pseudo network adapter in the client and the pseudo network adapter in the server respectively. The reserved physical addresses should have a high likelihood of not being used in any actual network interface.

While the invention has been described with reference to specific example embodiments, the description is not meant to be construed in a limiting sense. Various modifications of the disclosed embodiments, as well as other embodiments of the invention, will be apparent to persons skilled in the art upon reference to this description. Specifically, while various embodiments have been described using the TCP/IP protocol stack, the invention may advantageously be applied where other communications protocols are used. Also, while various flow charts have shown steps performed in an example order, various implementations may use altered orders of step in order to apply the invention. And further, while certain specific software and/or hardware platforms

have been used in the description, the invention may be applied on other platforms with similar advantage. It is therefore contemplated that the appended claims will cover any such modifications or embodiments which fall within the scope of the invention.

Claims

1. A pseudo network adapter providing a virtual private network, comprising:

an interface for capturing packets from a local communications protocol stack for transmission on said virtual private network, said interface appearing to said local communications protocol stack as a network adapter device driver for a network adapter connected to said virtual private network;

a first server emulator, providing a first reply packet responsive to a first request packet captured by said interface for capturing packets from said local communications protocol stack for transmission on said virtual private network, said first request packet requesting a network layer address for said pseudo network adapter, said first reply indicating a network layer address for said pseudo network adapter; and a second server emulator, providing a second reply packet responsive to a second request packet captured by said interface for capturing packets from said local communications protocol stack for transmission on said virtual private network, said second request packet requesting a physical address corresponding to a network layer address of a second pseudo network adapter, said second pseudo network adapter located on a remote server node, said second reply indicating a predetermined, reserved physical address.

2. The pseudo network adapter of claim 1, further comprising a means for indicating to said local communications protocol stack that said predetermined, reserved physical address is reachable through said pseudo network adapter, wherein said means for indicating modifies a data structure in said local communications protocol stack indicating which nodes or networks are reachable through each network interface of the local system.

3. The pseudo network adapter of claim 1, further comprising a means for indicating to said local communications protocol stack that one or more nodes on a remote private network connected to said remote server node are reachable through a gateway node equal to said second pseudo network adapter on said remote server node.

- 4. The pseudo network adapter of claim 1, further comprising:

a transmit path for processing data packets captured by said interface for capturing packets from said local communications protocol stack for transmission on said virtual private network; an encryption engine, within said transmit path, for encrypting said data packets; an encapsulation engine, within said transmit path, for encapsulating said encrypted data packets into tunnel data frames; and a means for passing said tunnel data frames back to said local communications protocol stack for transmission to a physical network adapter on said remote server node.

- 5. The pseudo network adapter of claim 4, wherein said transmit path further includes means for storing a digest value in a digest field in each of said tunnel data frames, said digest value equal to an output of a keyed hash function applied to said data packet encapsulated within said tunnel data frame concatenated with a counter value equal to a total number of tunnel data frames previously transmitted to said remote server node.

- 6. The pseudo network adapter of claim 4, wherein said transmit path further includes means for processing an Ethernet header in each one of said captured data packets, said processing of said Ethernet header including removing said Ethernet header.

- 7. The pseudo network adapter of claim 1, further comprising:

an interface into a transport layer of said local communications protocol stack for capturing received data packets from said remote server node.

- 8. The pseudo network adapter of claim 7, further comprising:

a receive path for processing received data packets captured by said interface into said transport layer of said local communications protocol stack for capturing received data packets from said remote server node; an decapsulation engine, within said receive path, for decapsulating said received data packets by removing a tunnel frame header; an decryption engine, within said receive path, for decrypting said received data packets; and a means for passing said received data packets back to said local communications protocol stack for delivery to a user.

- 9. A method for providing a pseudo network adapter for a virtual private network, comprising the steps of:

capturing packets from a local communications protocol stack for transmission on said virtual private network, said capturing through an interface appearing to said local communications stack as a network adapter device driver for a network adapter connected to said virtual private network; issuing a first reply packet responsive to a first request packet captured by said interface for capturing packets from said local communications protocol stack for transmission on said virtual private network, said first request packet requesting a network layer address for said pseudo network adapter, said first reply indicating a network layer address for said pseudo network adapter; and issuing a second reply packet responsive to a second request packet captured by said interface for capturing packets from said local communications protocol stack for transmission on said virtual private network, said second request packet requesting a physical address corresponding to a network layer address of a second pseudo network adapter, said second pseudo network adapter located on a remote server node, said ARP Reply indicating a predetermined, reserved physical address.

- 10. The method of claim 9, further comprising indicating to said local communications protocol stack that said predetermined, reserved physical address is reachable through said pseudo network adapter, wherein said step of indicating to said local communications protocol stack modifies a data structure in said local communications protocol stack indicating which nodes or networks are reachable through each network interface of the local system.

- 11. The method of claim 9, further comprising indicating to said local communications protocol stack that one or more nodes on a remote private network connected to said remote server node are reachable through a gateway node equal to said second pseudo network adapter on said remote server node, wherein said step of indicating to said local communications protocol stack that one or more nodes on said remote private network connected to said remote server node are reachable through a gateway node equal to said second pseudo network adapter on said remote server node modifies a network layer routing table in said local communications protocol stack.

- 12. The method of claim 9, further comprising:

processing data packets captured by said interface for capturing packets from said local communications protocol stack for transmission on said virtual private network in a transmit data path;

5

encrypting said data packets in an encryption engine, within said transmit path;
 encapsulating said encrypted data packets into tunnel data frames by an encapsulation engine, within said transmit path; and
 passing said tunnel data frames back to said local communications protocol stack for transmission to a physical network adapter on said remote server node, wherein said transmit path further includes storing a digest value in a digest field in each of said tunnel data frames, said digest value equal to an output of a keyed hash function applied to said data packet encapsulated within said tunnel data frame concatenated with a counter value equal to a total number of tunnel data frames previously transmitted to said remote server node.

10

15

20

13. The method of claim 12, wherein said transmit path further includes processing an Ethernet header in each one of said captured data packets, said processing of said Ethernet header including removing said Ethernet header.

25

14. The method of claim 9, further comprising capturing received data packets from said remote server node through an interface into a transport layer of said local communications protocol stack, further comprising:

30

35

processing received data packets captured by said interface into said transport layer of said local communications protocol stack for capturing received data packets from said remote server node in a receive path;
 decapsulating said received data packets by removing a tunnel frame header in an decapsulation engine, within said receive path;
 decrypting said received data packets in a decryption engine within said receive path; and
 passing said received data frames packets back to said local communications protocol stack for delivery to a user.

40

45

15. The method of claim 9, wherein said network layer address for said pseudo network adapter and said predetermined, reserved physical address is communicated to said pseudo network adapter from said remote server node as client data in a connection response frame.

50

55

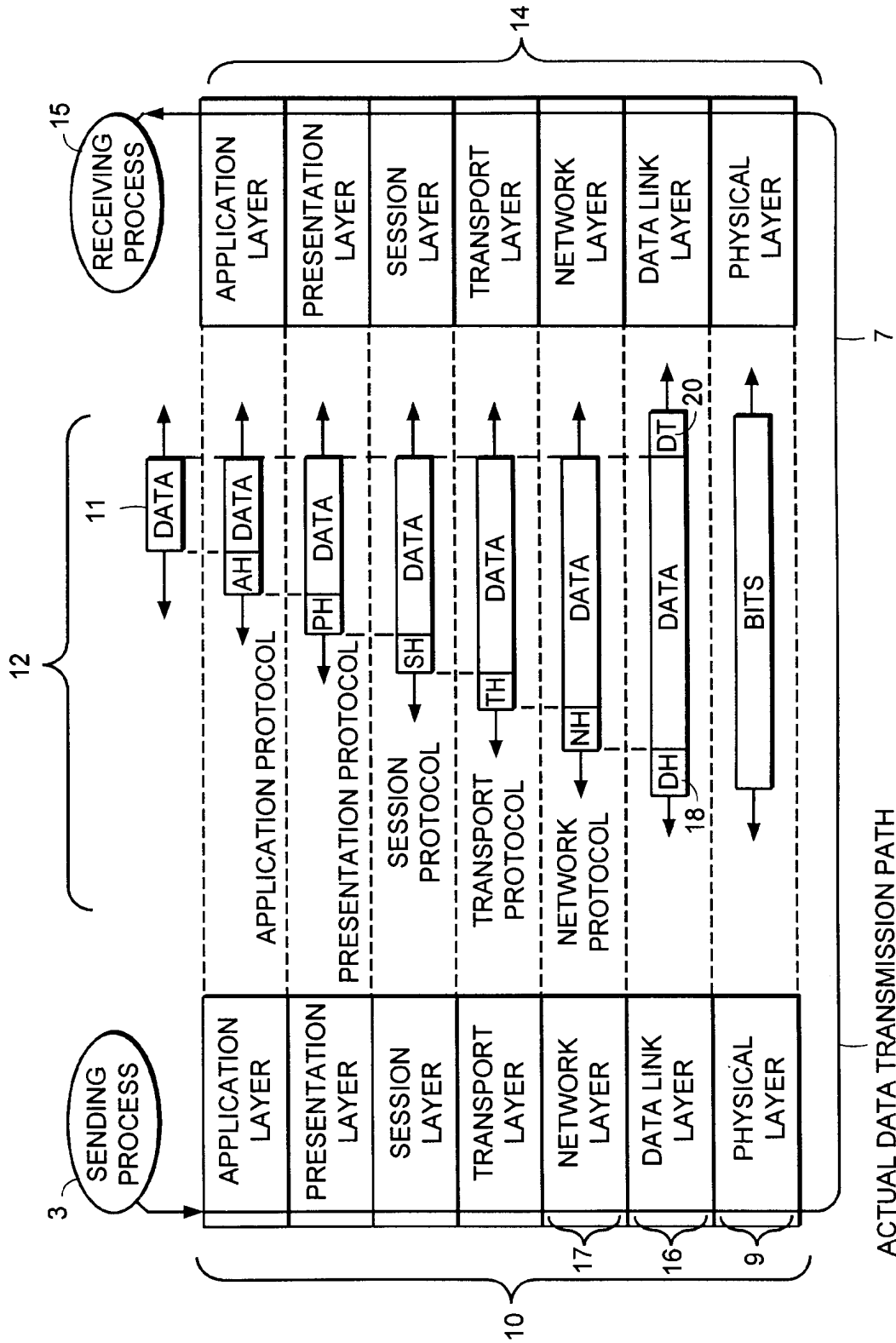


FIG. 1

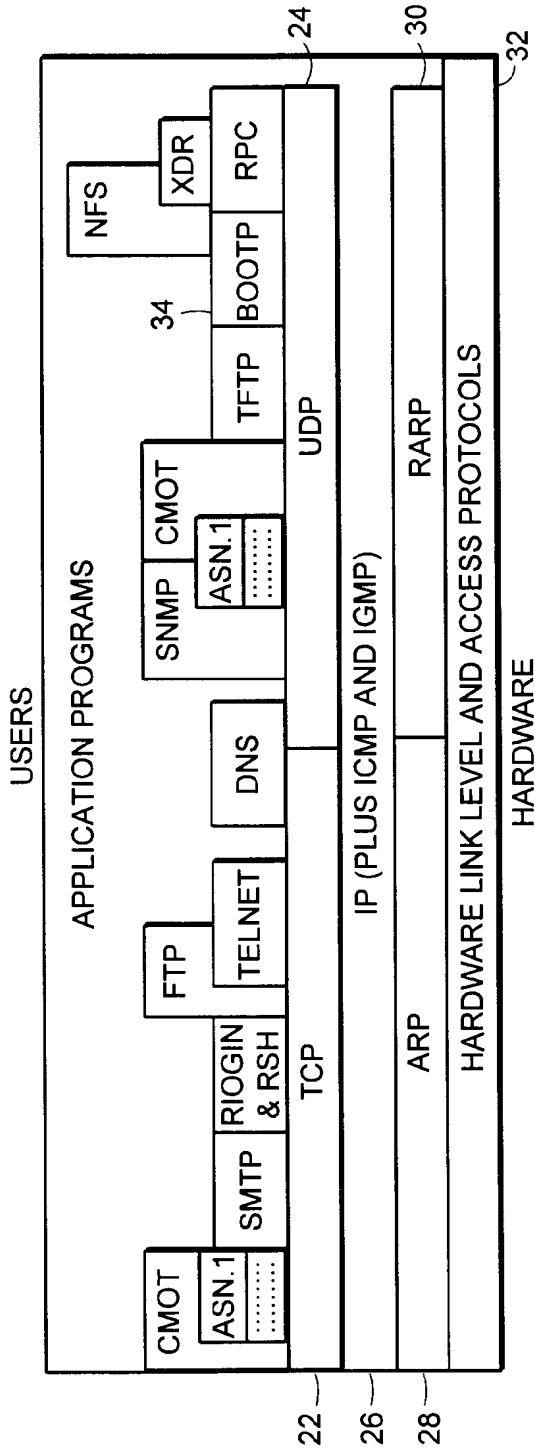


FIG. 2

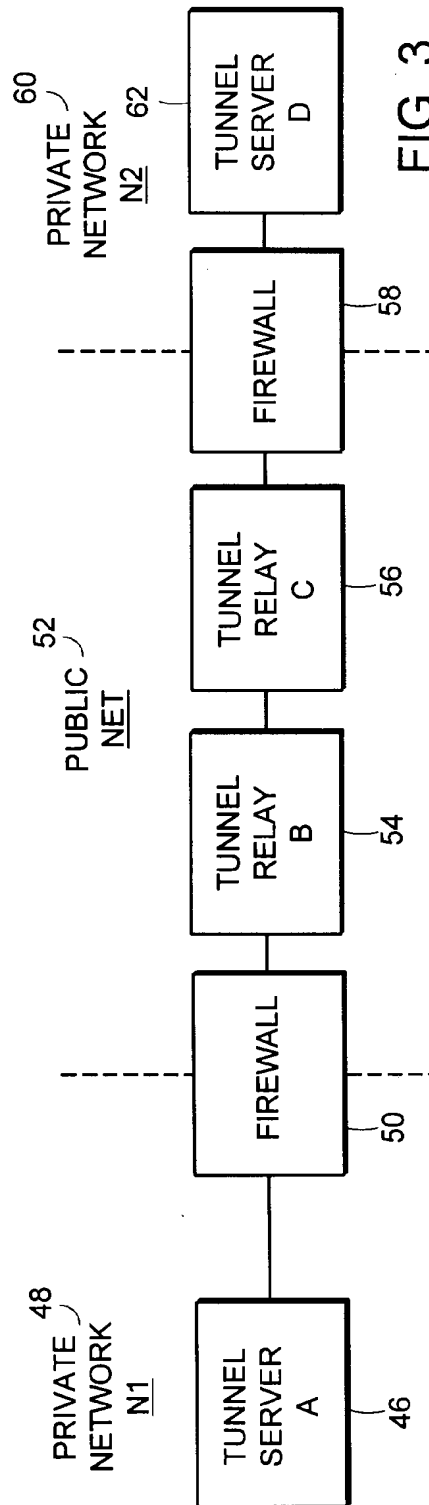


FIG. 3

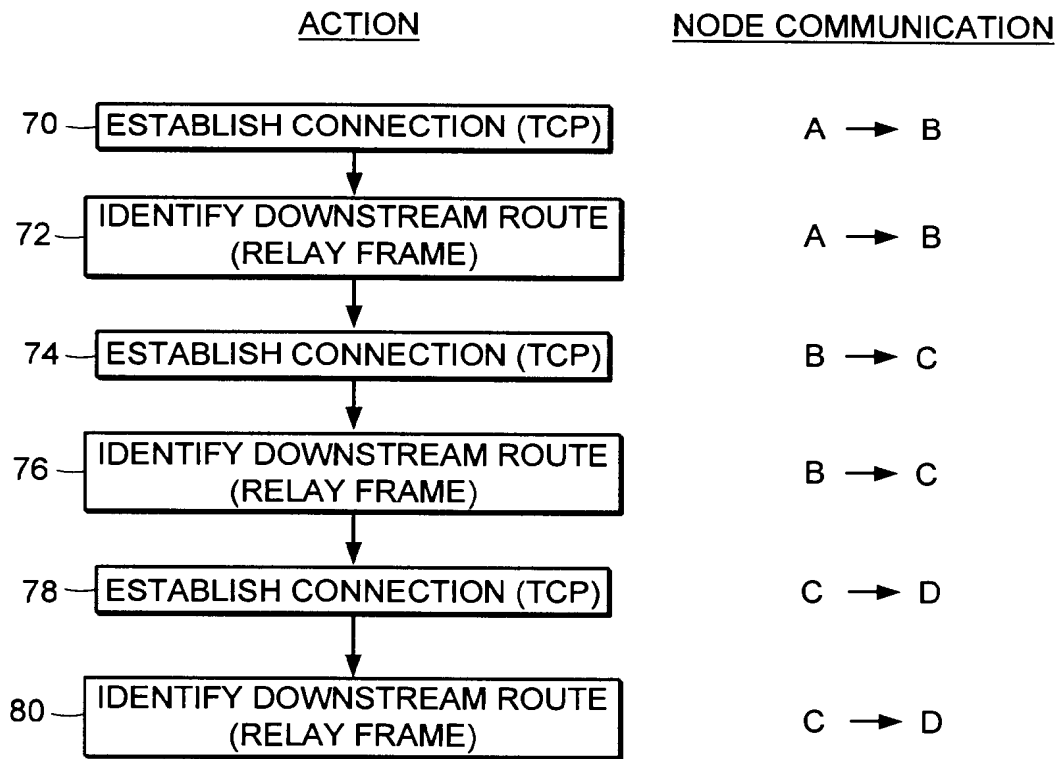


FIG. 4

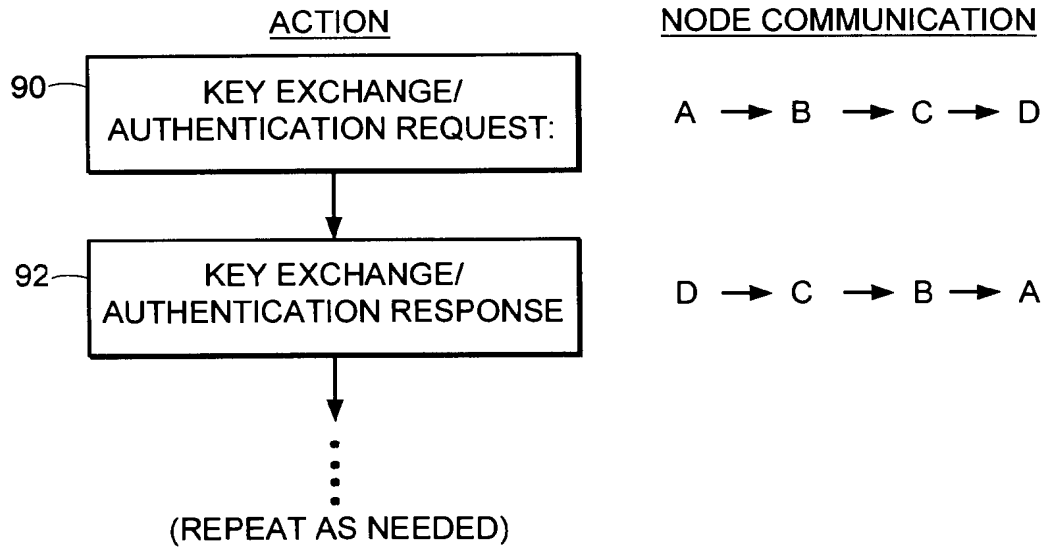


FIG. 5

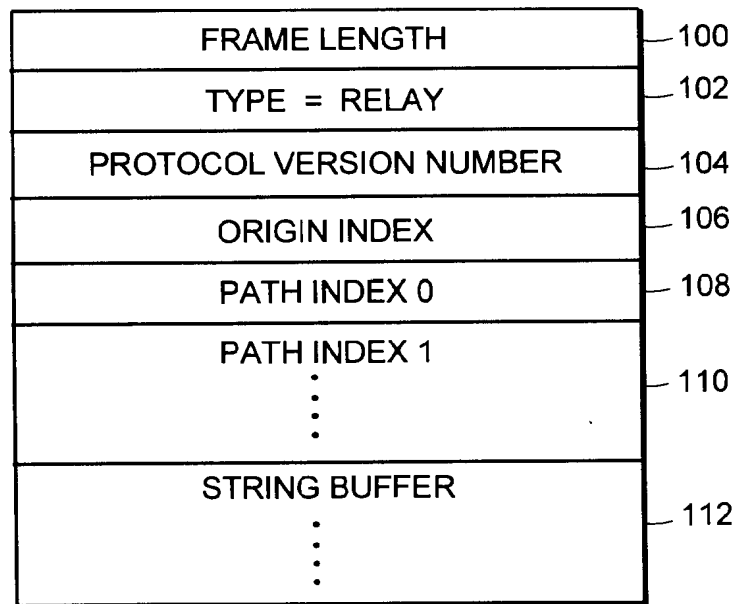


FIG. 6

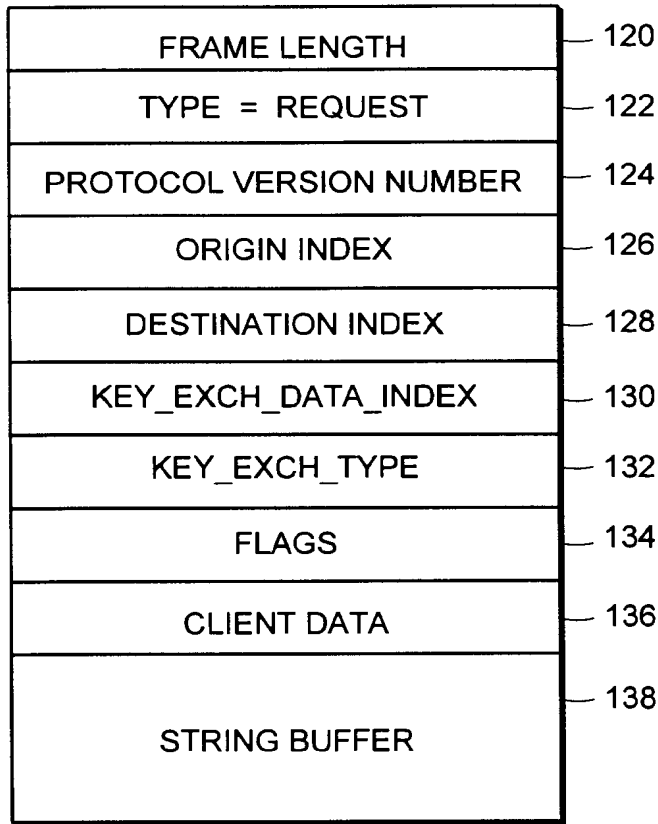


FIG. 7

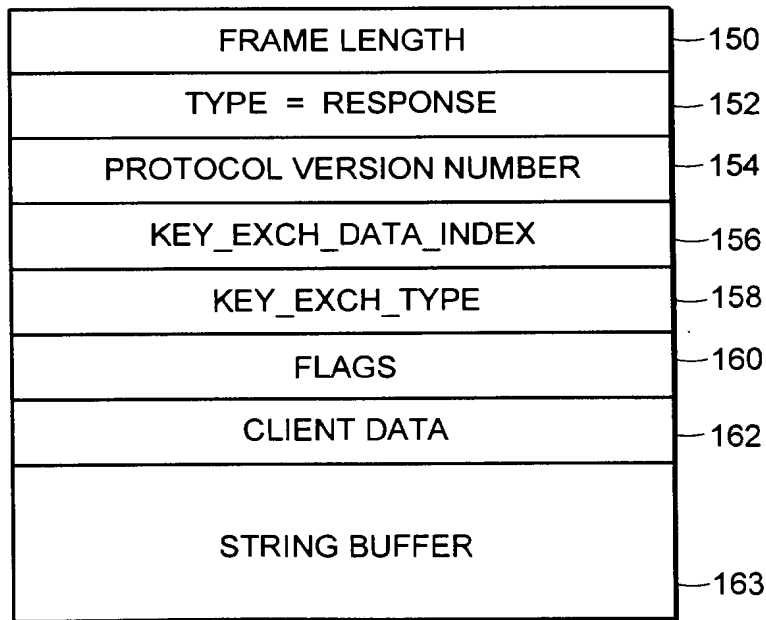


FIG. 8

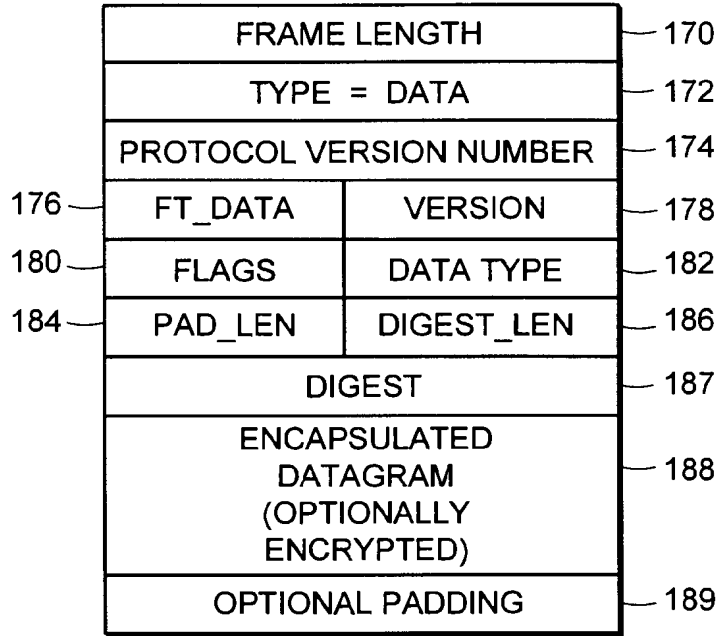


FIG. 9

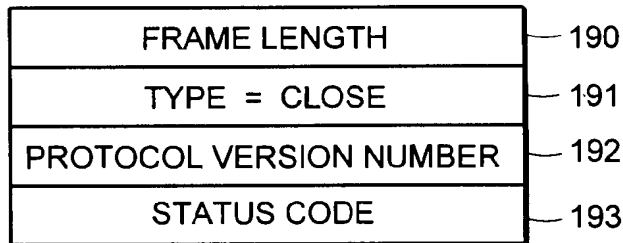


FIG. 10

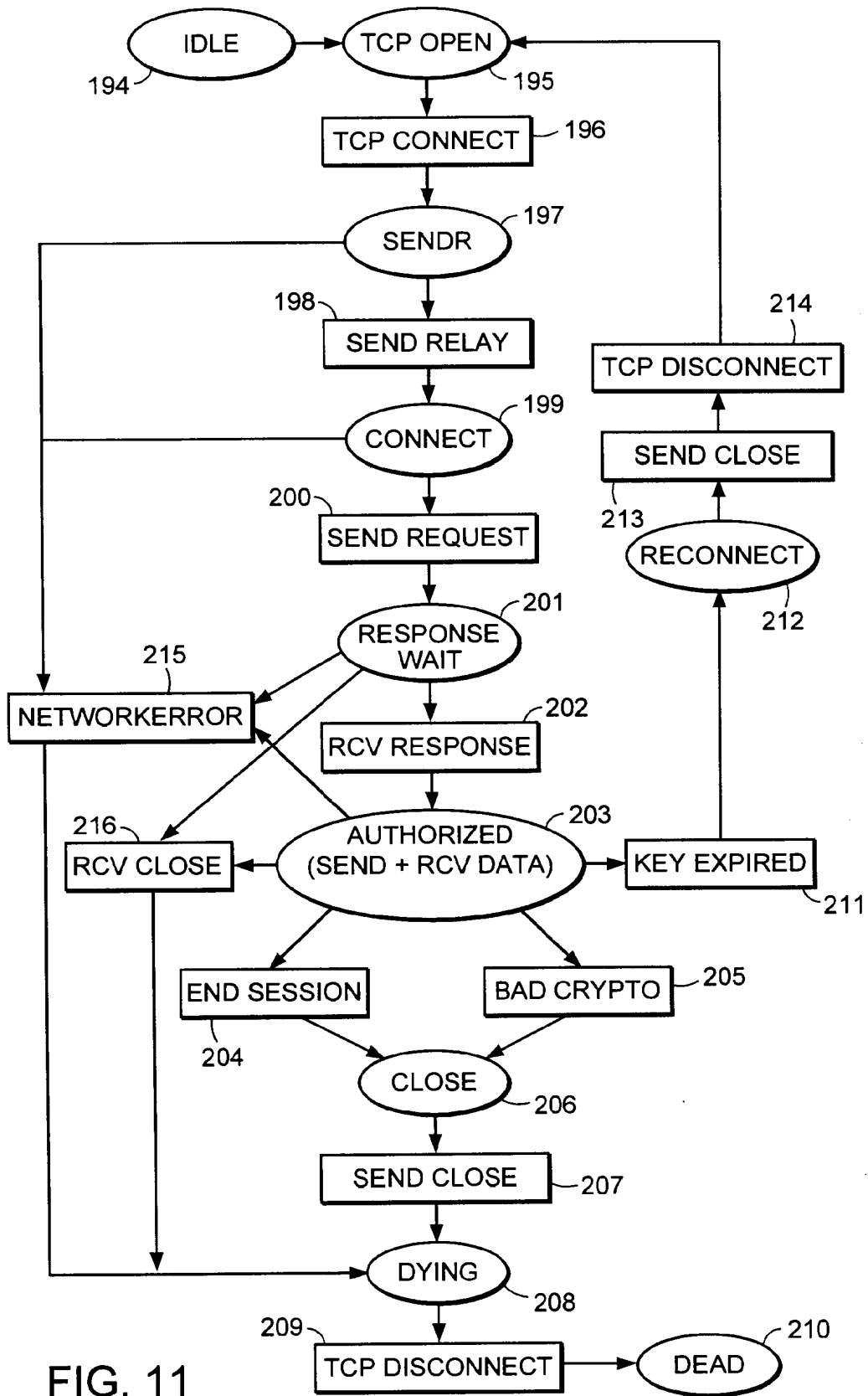


FIG. 11

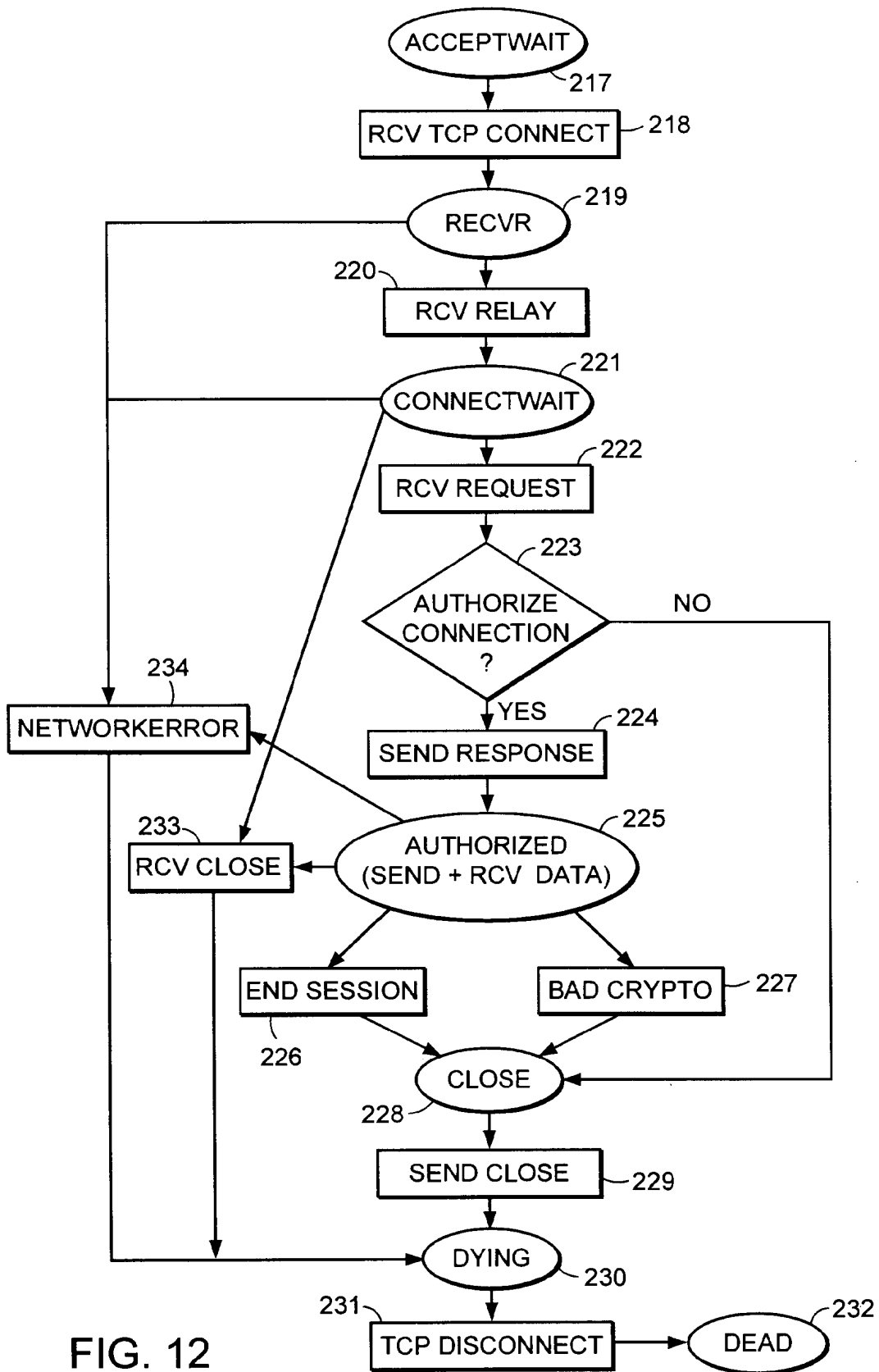


FIG. 12

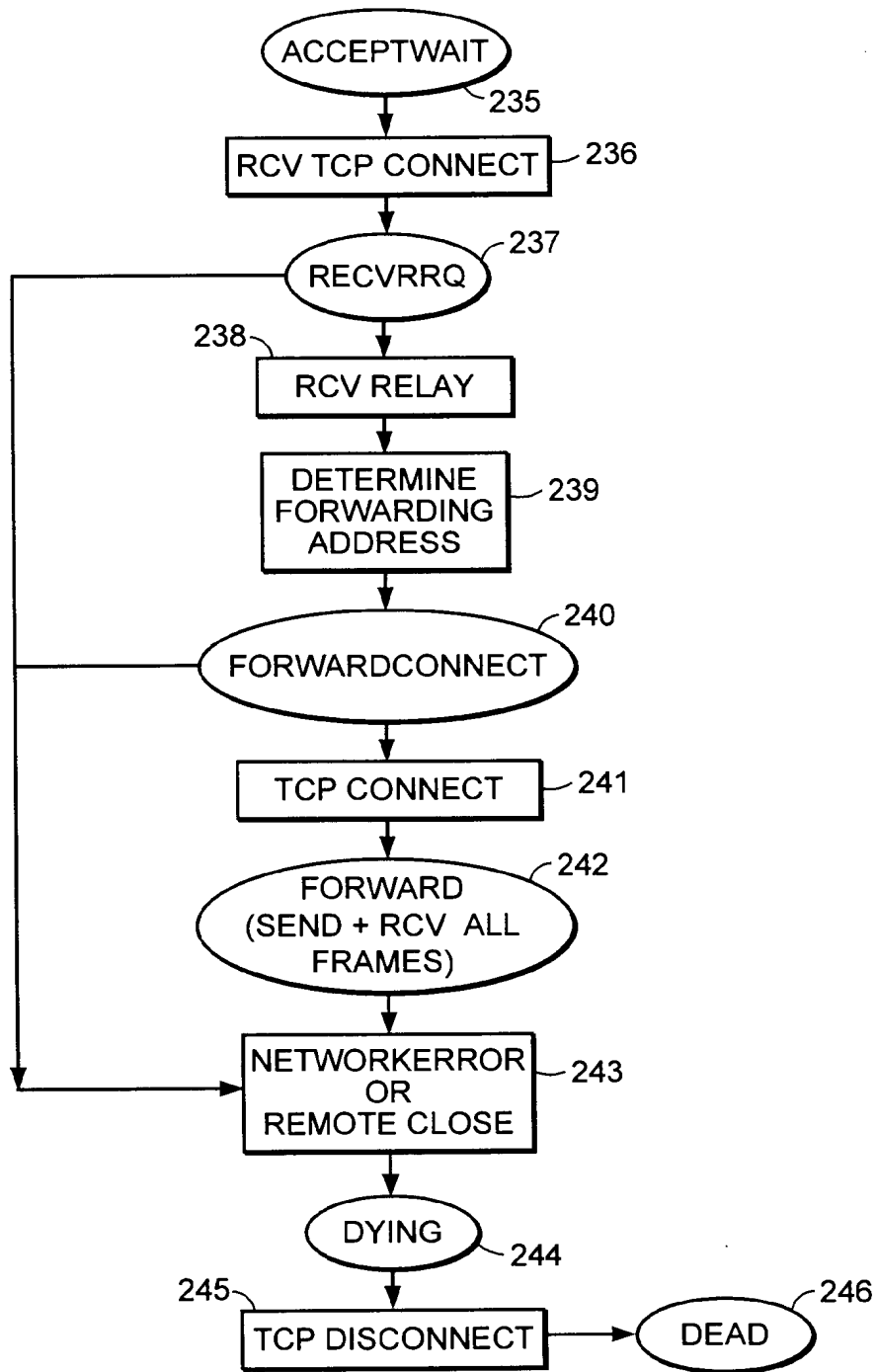


FIG. 13

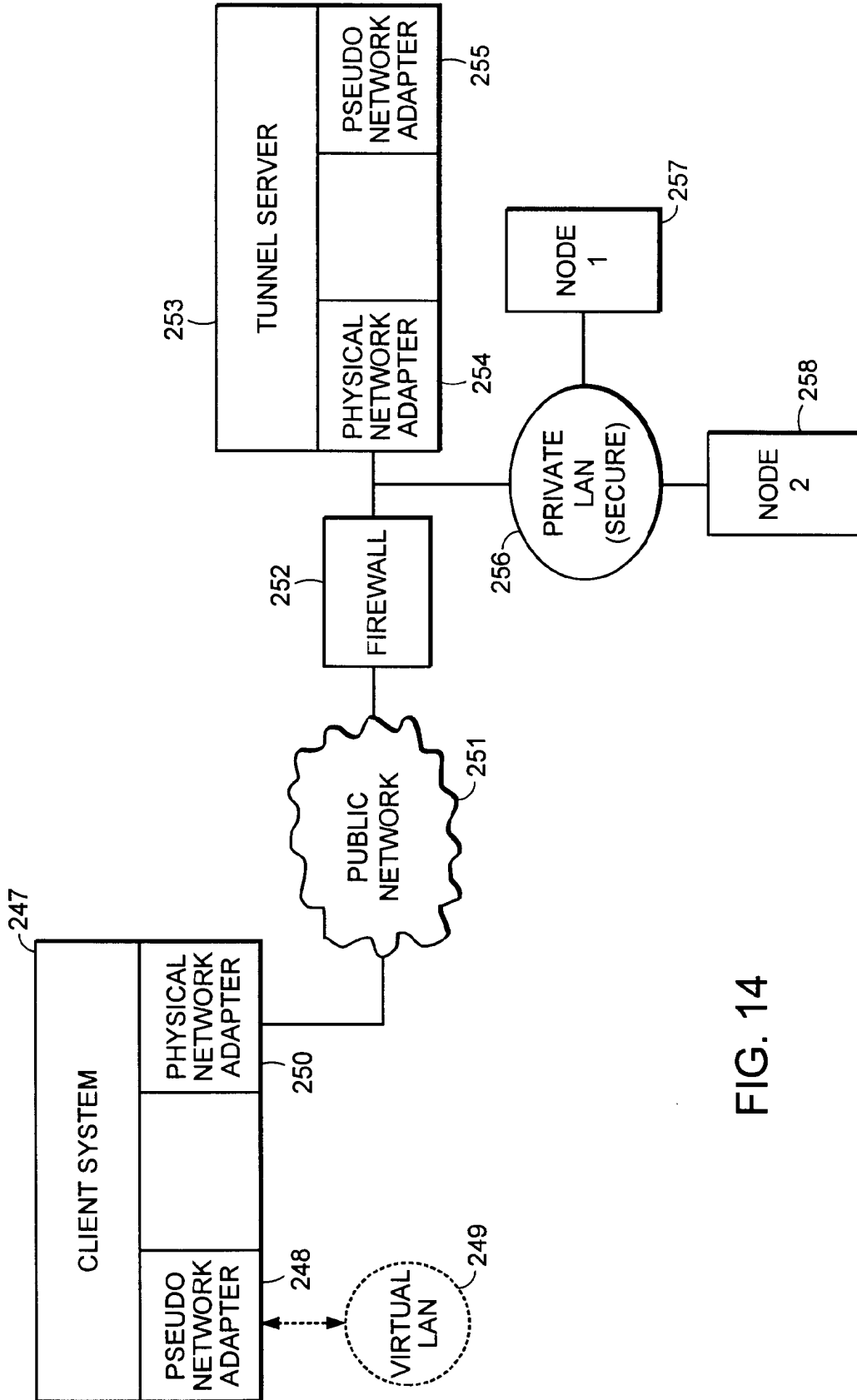


FIG. 14

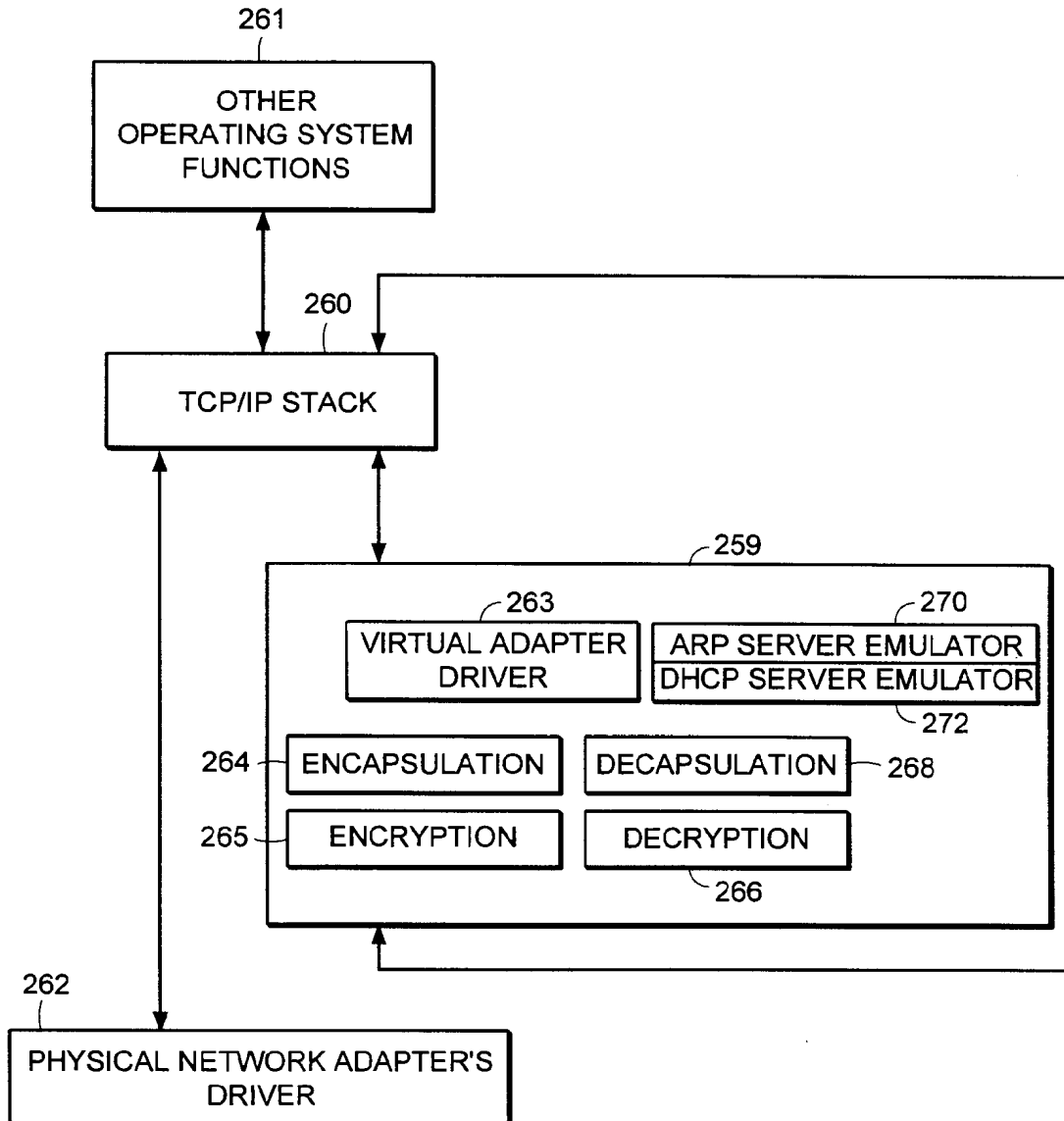


FIG. 15

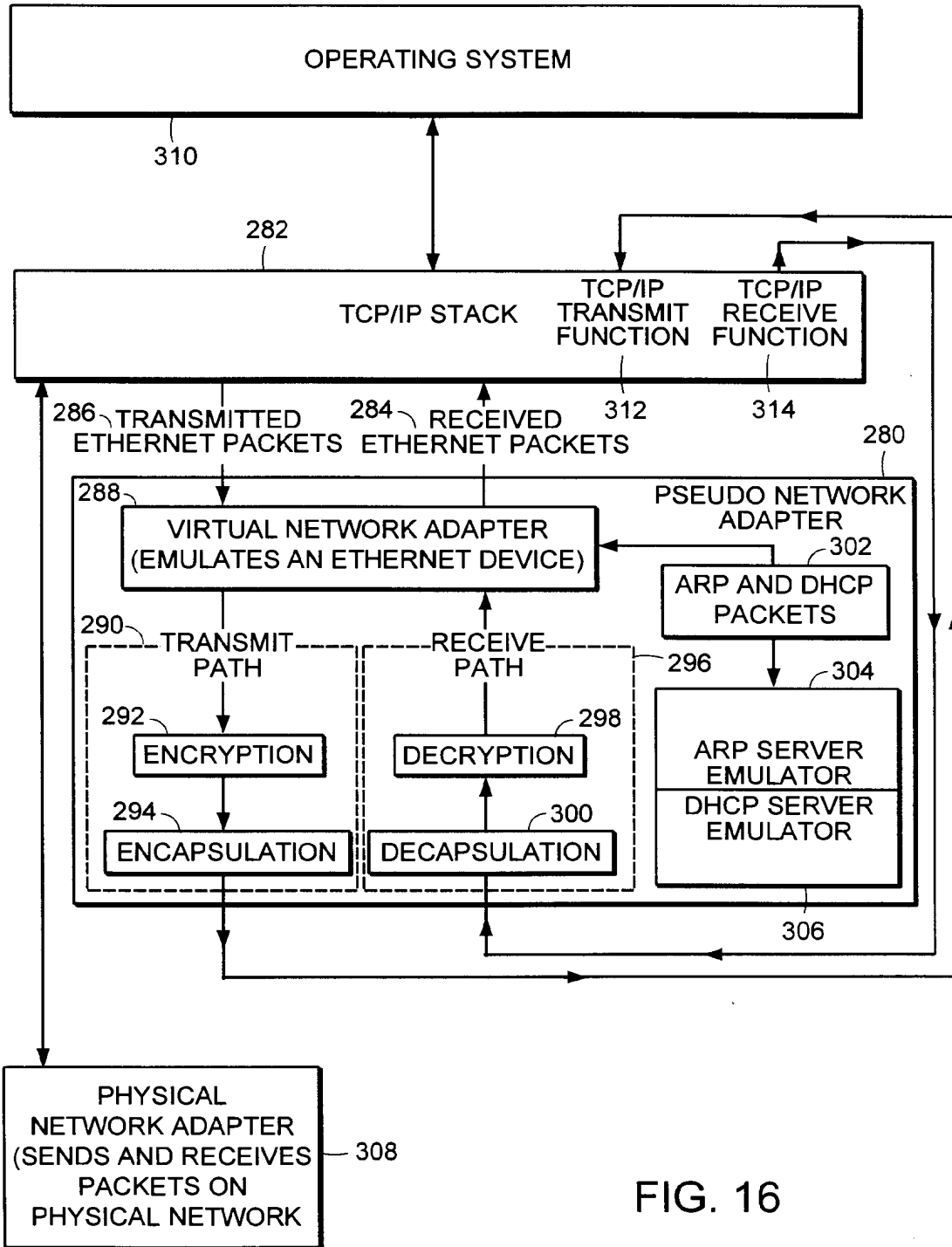


FIG. 16

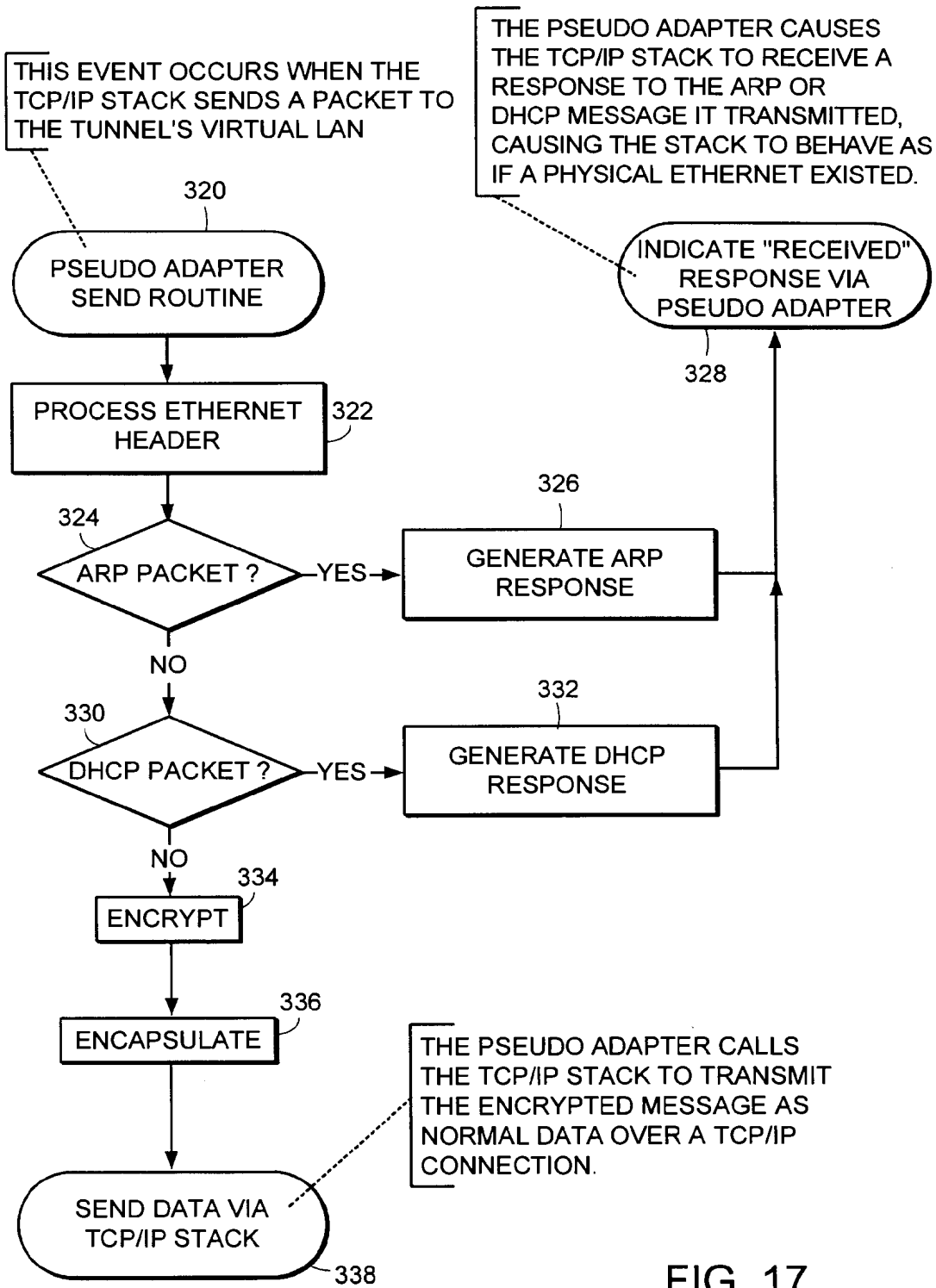


FIG. 17

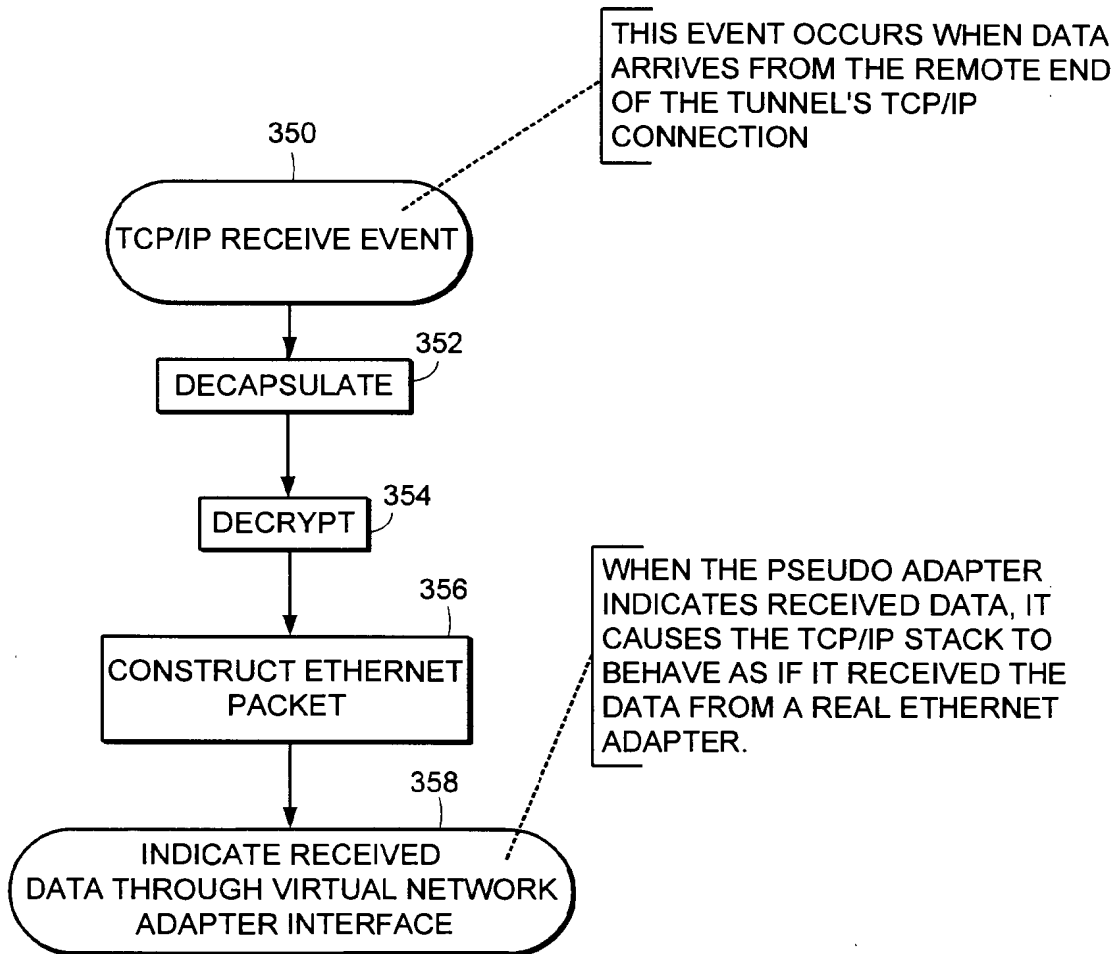


FIG. 18

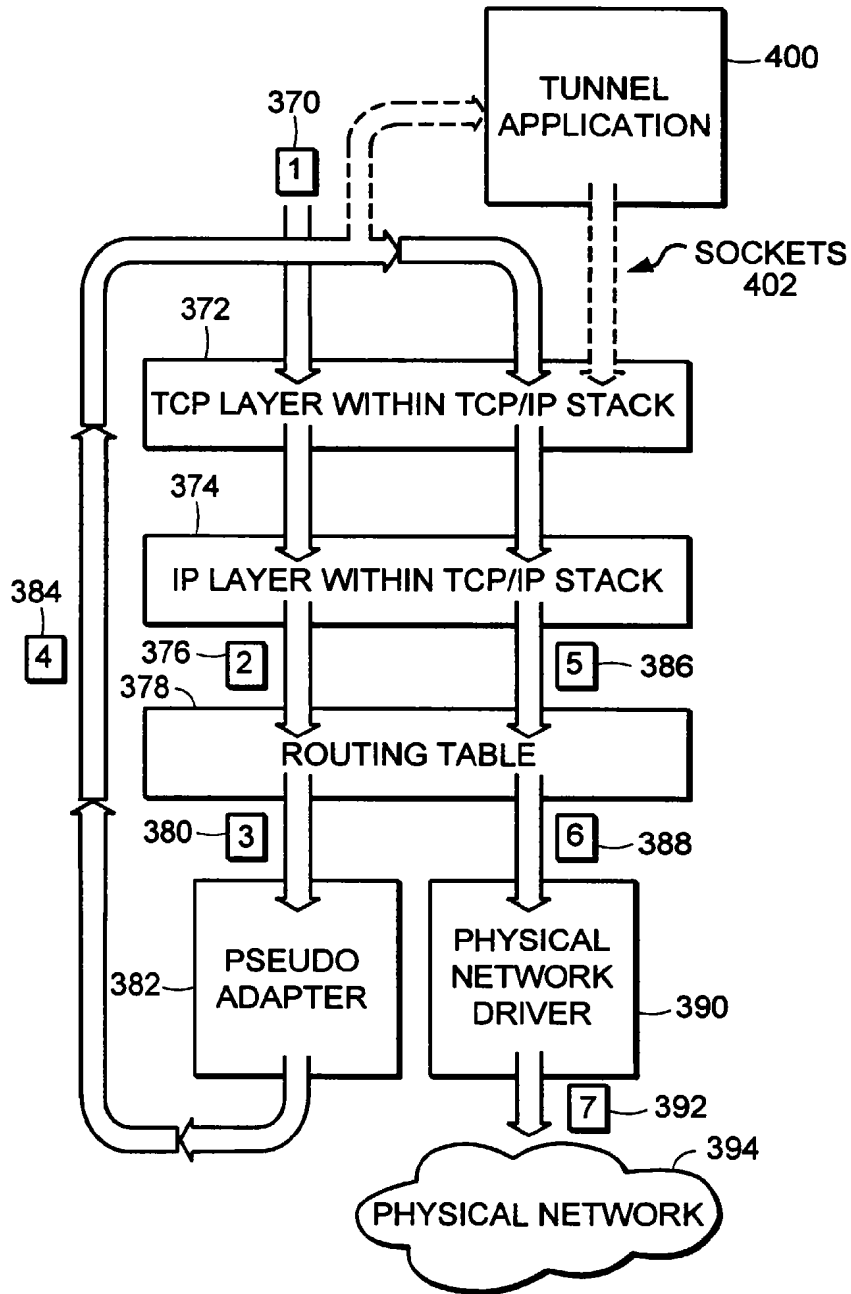


FIG. 19

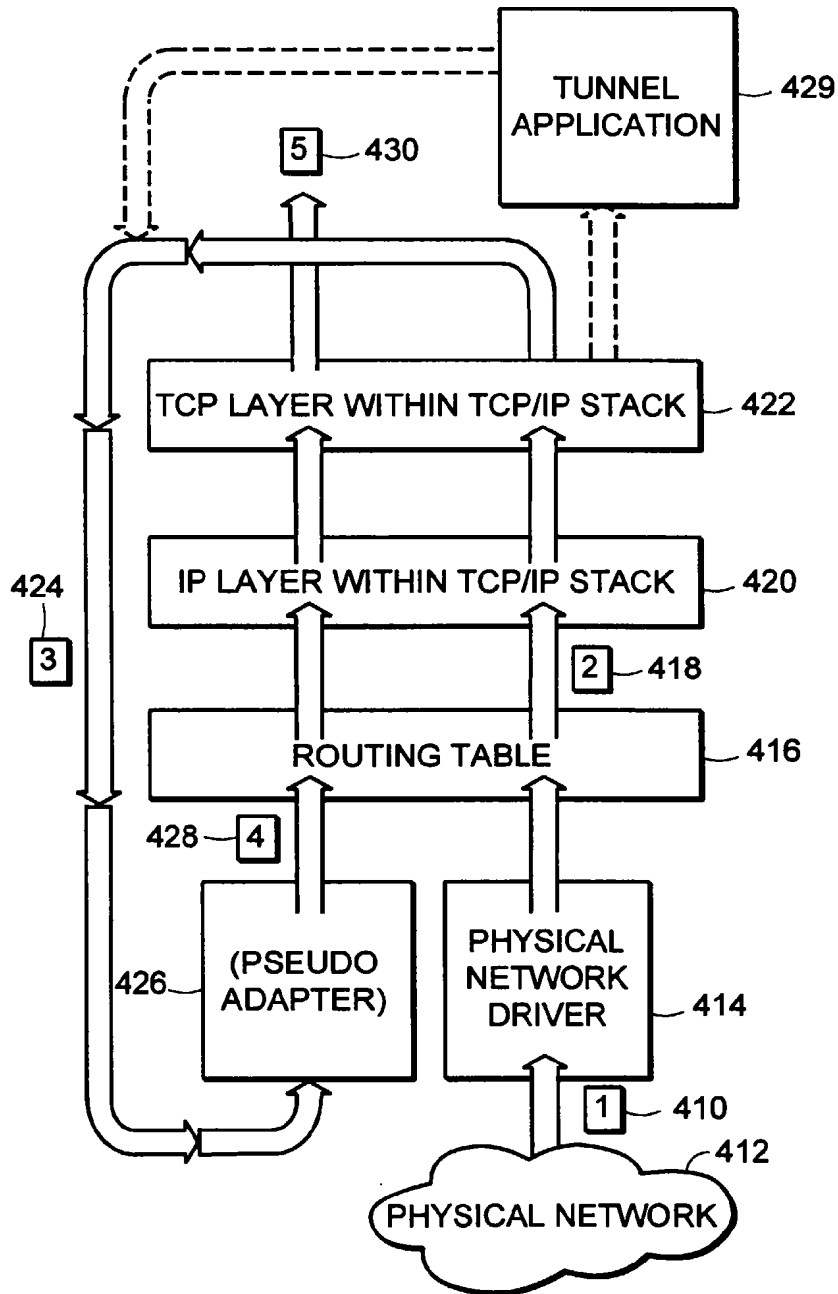


FIG. 20

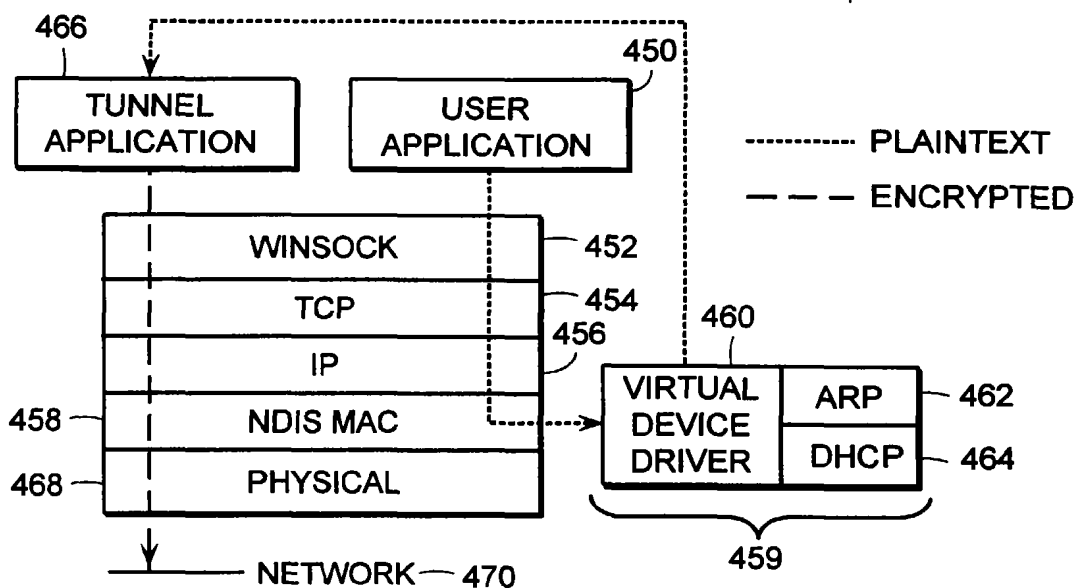


FIG. 21

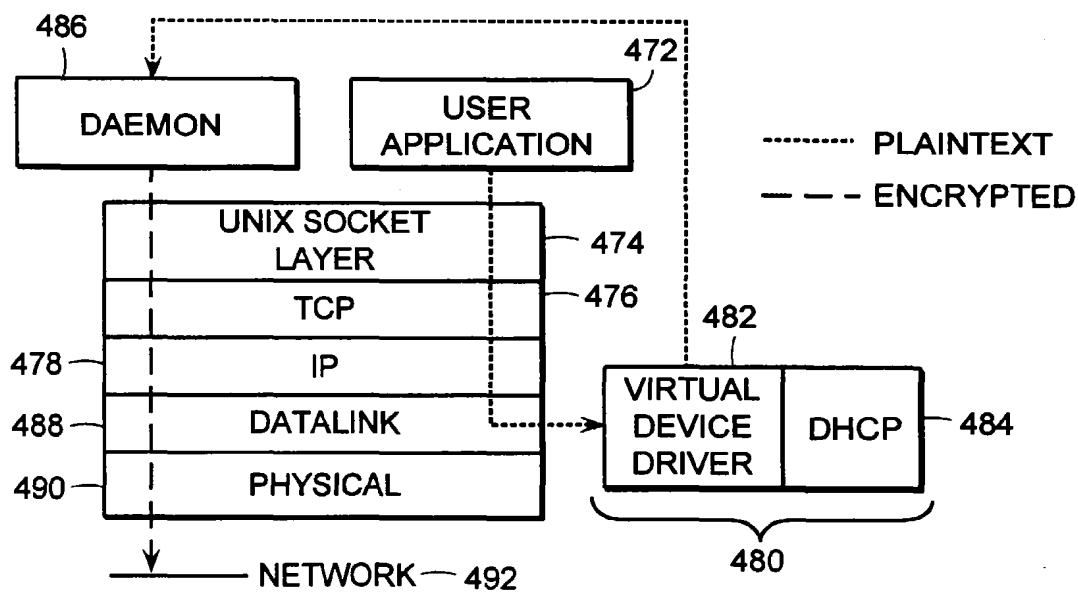


FIG. 22

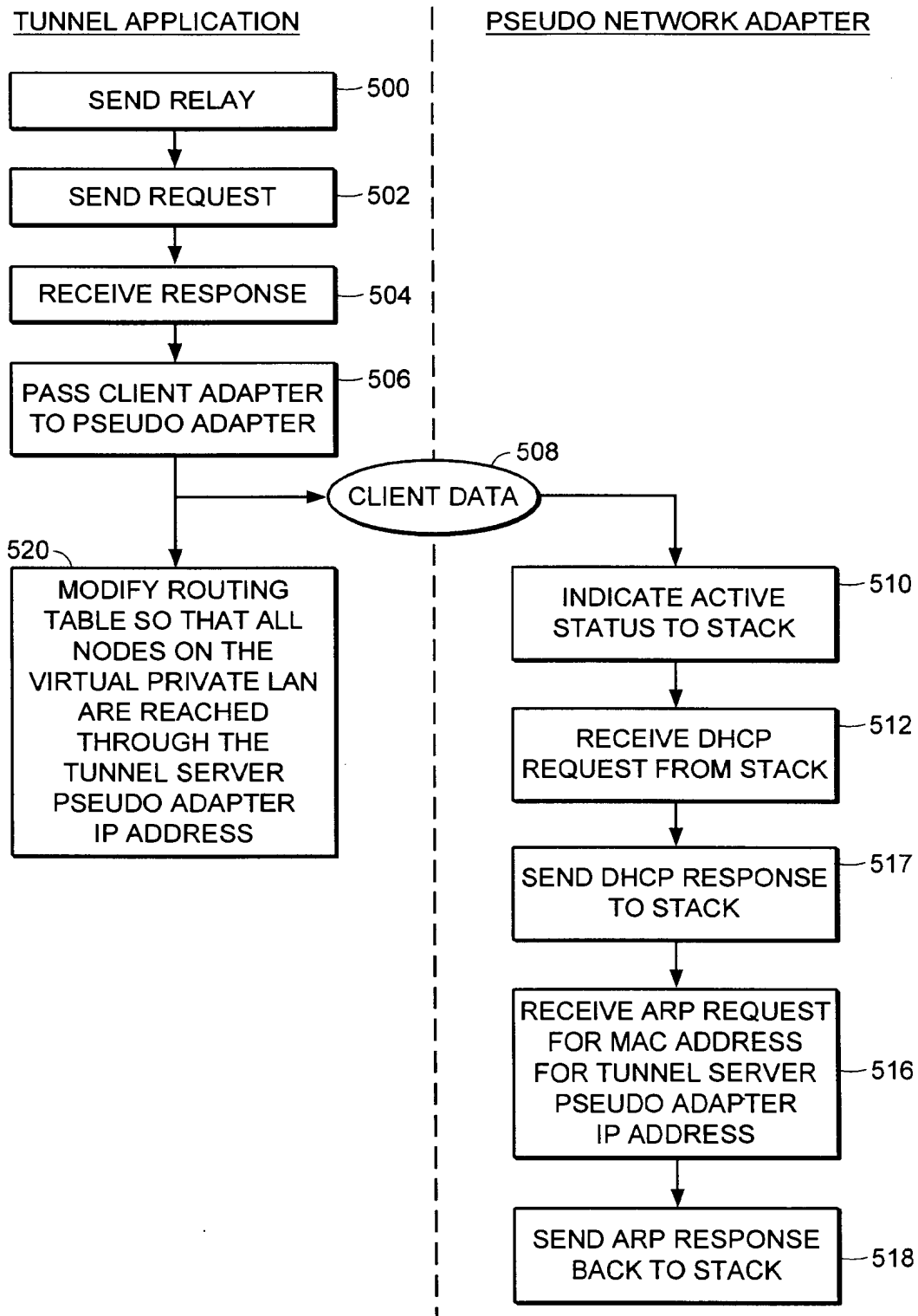
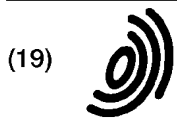


FIG. 23



Europäisches Patentamt

(19)

European Patent Office

Office européen des brevets



(11)

EP 0 814 589 A2

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:
29.12.1997 Bulletin 1997/52

(51) Int. Cl.⁶: H04L 29/06

(21) Application number: 97109792.8

(22) Date of filing: 16.06.1997

(84) Designated Contracting States:
AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL
PT SE

- Kimmeth, Thomas
Gladstone, N.J. 07977 (US)
- Nusbaum, Kurt
Downers Grove, Illinois 60515 (US)

(30) Priority: 19.06.1996 US 667524

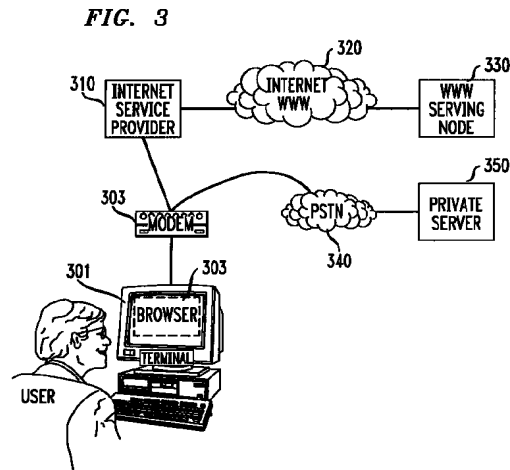
(71) Applicant: AT&T Corp.
New York, NY 10013-2412 (US)

(74) Representative:
KUHNNEN, WACKER & PARTNER
Alois-Steinecker-Strasse 22
85354 Freising (DE)

(72) Inventors:
• Harwood, Jonathan P.
Morganville, N.J. 07751 (US)

(54) System and method for automated network reconfiguration

(57) A method is disclosed for providing an enhanced level of security for sensitive or proprietary information associated with information transactions in a public network, such as the Internet. In carrying out that method, an on-line information transaction is bifurcated between a generalized information access portion of such a transaction and an exchange of sensitive user information. With such a bifurcation, the generalized information access portion of the transaction, which generally would constitute the more substantial (in terms of network resources) portion of the transaction, would be handled via a non-secure network, usually a public network such as the Internet. The portion of the transaction involving sensitive user information, on the other hand, would be handled by a separate secure connection, such as a private network, or intranetwork. An important characteristic of this bifurcation arrangement is the provision of a means for automated reconfiguration of a user terminal as between accessing the generalized information via the non-secure network and access to the secure communications network for the exchange of sensitive user information. Such an automated reconfiguration will be carried out without the necessity for any action on the part of the user, and indeed will be largely invisible to the user.



EP 0 814 589 A2

Description

FIELD OF THE INVENTION

5 This invention is related to the field of data communications, and more particularly to a method and means for establishing an automatic reconfiguration of a user terminal among alternative tasks.

BACKGROUND OF THE INVENTION

10 With the increasing popularity of personal computers over the last several years has come a striking growth in transaction-oriented computer-to-computer communications (as opposed to bulk-data transfers among such computers). For convenience herein such transaction-oriented computer-to-computer communications will be described by the shorthand term "information transaction". That growth in the use of computers for such information transactions has unquestionably been fueled by the existence of an international infrastructure for implementing such data communications, known as the Internet. And, driven by the burgeoning demand for such information transaction services, the Internet has itself experienced explosive growth in the amount of traffic handled.

15 At least partly in response to that demand, a new level of accessibility to various information sources has recently been introduced to the Internet, known as the World Wide Web ("WWW"). The WWW allows a user to access a universe of information which combines text, audio, graphics and animation within a hypermedia document. Links are contained within a WWW document which allow simple and rapid access to related documents. Using a system known as the HyperText Markup Language ("HTML"), pages of information in the WWW contain pointers to other pages, those pointers typically being a key word (commonly known as a hyperlink word). When a user selects one of those key words, a hyperlink is created to another information layer (which may be in the same, or a different information server), where typically additional detail related to that key word will be found.

20 In order to facilitate implementation of the WWW on the Internet, new software tools have been developed for user terminals, usually known as Web Browsers, which provide a user with a graphical user interface means for accessing information on the Web, and navigating among information layers therein. A commonly used such Web Browser is that provided by Netscape.

25 The substantial growth in the use of computer networks, and particularly the WWW, for such information transactions, has predictably led to significant commercialization of this communications medium. For example, with the WWW, a user is not only able to access numerous information sources, some public and some commercial, but is also able to access "catalogs" of merchandise, where individual items from such a catalog can be identified and ordered, and is able to carry out a number of banking and other financial transactions. As will be obvious, such commercial transactions will typically involve sensitive and proprietary information, such as credit card numbers and financial information of a user. Thus, with the growth of commercial activity in the Internet, has also come a heightened concern with security.

30 It is well known that there are persons with a high level of skill in the computer arts, commonly known as "hackers", who have both the ability and the will to intercept communications via the Internet. Such persons are thereby able to gain unauthorized access to various sensitive user information, potentially compromising or misappropriating such information.

35 The vulnerability of such sensitive user information to misuse when so transmitted via the Internet is a phenomena which has only recently received wide public attention. Unless such security concerns can be quickly addressed and alleviated, the commercial development of this new communications medium may be slowed or even stalled altogether.

SUMMARY OF THE INVENTION

40 Accordingly, it is an object of the invention to provide an acceptable level of security for sensitive or proprietary information associated with information transactions in a public network, such as the Internet. That object is realized through an arrangement whereby an on-line information transaction is bifurcated between a generalized information access portion of such a transaction and an exchange of sensitive user information. With such a bifurcation, the generalized information access portion of the transaction, which generally would constitute the more substantial (in terms of network resources) portion of the transaction would be handled via a non-secure network, usually a public network such as the Internet. The portion of the transaction involving sensitive user information, on the other hand, would be handled by a separate secure connection, such as a private network, or intranetwork. An important characteristic of this bifurcation arrangement is the provision of a means for automated reconfiguration of a user terminal as between accessing the generalized information via the non-secure network and access to the secure communications network for the exchange of sensitive user information. Such an automated reconfiguration will be carried out without the necessity for any action on the part of the user, and indeed will be largely invisible to the user. In a further embodiment of the invention, a transfer of data is provided from a public to a private network, wherein data selected by a user from a public net-

work site may be arranged and displayed at a user terminal and, subject to further user selection/confirmation activity, thereafter transferred to a private network.

BRIEF DESCRIPTION OF THE DRAWINGS

5

Figure 1 depicts an illustrative case of information transactions carried out via a public network such as the Internet.

Figure 2 shows the architecture of a browser as would typically be applied for accessing a hypermedia web page.

Figure 3 illustrates the primary elements of the reconfigurable dual-path method of the invention.

Figure 4 depicts in flow chart form the basic jump capability of the methodology of the invention.

10

Figures 5A & 5B (generally designated collectively herein as "Figure 5") depict in flow chart form the "shopping cart" capability of the methodology of the invention.

Figure 6A & 6B (generally designated collectively herein as "Figure 6") depict in flow chart form the stored configuration capability of the methodology of the invention.

15

Figure 7A & 7B (generally designated collectively herein as "Figure 7") depict in flow chart form the off-line form capability of the methodology of the invention.

DETAILED DESCRIPTION

20

For clarity of explanation, the illustrative embodiment of the present invention is presented as comprising individual functional blocks. The functions these blocks represent may be provided through the use of either shared or dedicated hardware, including, but not limited to, hardware capable of executing software.

25

Figure 1 depicts an illustrative case of information transactions carried out via the Internet. As seen in the figure, an exemplary user obtains access to the Internet by first connecting, via a Terminal 110 having an associated Browser 111, to an Internet Service Provider 112 selected by the user. That connection between the user and the Internet Service Provider will typically be made via the Public Switched Telephone Network (PSTN) from a modem associated with the user's Terminal to a network node in the Internet maintained by the selected Internet Service Provider.

30

Once the user has obtained access to the selected Internet Service Provider, an address is provided for connection to another user or other termination site and such a connection is made via the Internet to that destination location. As can be seen from the figure, communication via the Internet may be either user-to-user, as from Terminal 110 to Terminal 130, or from a user to a node representing an information source accessed via the Internet, such as Public Site 120.

35

It will of course be understood that the Internet provides service to a large number of users and includes a large number of such Public Sites, but the illustration provides the essential idea of the communication paths established for such Internet communication. It will also be understood that a number of service classifications are supported by the Internet, with the World Wide Web service, which represents a preferred embodiment for the public network aspect of the method of the invention, being one of the currently most heavily trafficked of such services.

40

The Web Browser, such as depicted at 111, can be seen as a software application operating in conjunction with a user terminal (such as Terminal 110) which provides an interface between such a user terminal and the particular functionality of the WWW information site. The architecture of such a browser is generally described in terms of three main components, as illustrated in Figure 2. At the top level is the Browser 201, which enables the acquisition of information pages from a WWW server (beginning, in all cases, with the "home page" for that server), for display at a display device associated with the terminal. The Browser also provides the necessary interface for the terminal with the HTML functionality used by the server to provide access to other linked information layers.

45

The second level of the browser architecture is the TCP/IP Stack 202, which handles the communications protocols used for connecting the terminal to the WWW server. The bottom level of this architecture is the Dialer 203, which typically handles the function of providing dialing and setup digits to a modem, as illustrated at 204, such a modem generally being a part of the terminal. Normally, upon receiving dialing and other setup information from the dialer, the modem would cause a connection to be made via the PSTN to the Internet Service Provider selected for that terminal.

50

After a connection is established in this manner to the Internet Service Provider, an address would be provided for the WWW information node sought to be contacted, a connection to that node made through the Internet, and the home page for that node caused to be displayed at the terminal's display device. A user would then select a key word in that home page, typically by clicking on the word with a mouse or similar device, and, upon transmission of that selection signal to the WWW server, a hyperlink would be created to the linked information layer and the open page of that layer would be caused to be displayed at the user terminal.

55

As explained above, serious questions have been raised in respect to the security of communications via the public Internet. (Note, that the discussion herein is focused on the Internet, and particularly the WWW functionality of the Internet, as a preferred embodiment of such public data communication networks generally, but the methodology of the invention will be applicable to any such network.) To address this problem, the methodology of the invention begins with a bifurcation of the information transaction between a user and the selected information transaction provider into a por-

tion related to sensitive or proprietary user information, and other information comprising that transaction. With such a bifurcation, it becomes possible to provide substantial security for that proprietary information by use of an alternative communications path for that separated portion of the transaction via a private network, or intranetwork -- *i.e.*, a connection between a user's terminal and a secure serving node on that private network. It is anticipated that a coordination means will be established in respect to the management of information among the public and private network elements of the bifurcated information transaction.

In its basic form, this methodology may be carried out by the user terminal initiating a call via the Internet to a selected WWW node, and upon establishing connection to that node, proceeding with the desired information transaction up to the point where an exchange of sensitive or proprietary information were required. At that point the user terminal would be instructed by the WWW server to terminate that connection (*i.e.*, hangup) and to place a new call to an identified private network server for the necessary exchange of sensitive information.

However, in order to accomplish such a dual-path transaction, it is necessary that the browser at the user terminal be reconfigured to provide the dialing, authorization (*i.e.*, login and password), and other needed information for accessing the alternative private network, in order to implement the proprietary portion of the transaction. It will also usually be the case that, upon completion of that private-network transaction, the original dialer, stack and browser configurations will need to be restored, in order for the terminal to retain its normal Internet access functionality. Such a reconfiguration and subsequent restoral of the necessary parameters in the browser, stack and dialer is likely to be well beyond the capabilities of the average user.

Accordingly, as a further embodiment of the inventive methodology, an automated browser reconfiguration means is provided which interoperates with the browser. This browser reconfiguration means is described in detail hereafter and will be referred to as the "Bridging Software".

Figure 3 provides an illustration of the primary elements of the reconfigurable dual-path method of the invention. As seen in the figure, a first path comparable to the Internet link shown in Figure 1, between User Terminal 301 and WWW Serving Node 330 (via Browser 302, Modem 303, Internet Service Provider 310, and Internet 320) is provided. However, an alternative path is now provided from the output of Modem 303 to Private Server 350. That path is illustrated as being via the PSTN, which is generally regarded as being highly secure, but an alternative dedicated or other more-secure path between the User Terminal 301 and the Private Server 350 could as well be provided. In keeping with the discussion above, Browser 302 shown in Figure 3 would also include the Bridging Software installed as a helper application for implementing the automatic reconfiguration of the Browser.

In the operation of this system, a user would normally make an initial connection to an Internet application, such as the application represented by WWW Serving Node 330, which, *e.g.*, might be a shopping application, a financial transaction, or the provision of an enrollment form for off-line preparation. After conducting all, or some portion of an information transaction short of an exchange of sensitive or proprietary information, including a capture by the user's terminal of needed information from the public site, a user provides a signal indicative of an end to that portion of that transaction. During the course of the public portion of the information transaction, specially configured files are sent from the WWW serving node to the Bridging Software associated with Browser 302. Such files contain instructions for the Bridging Software to store information-like products -- *e.g.*, for selected items from a catalog, forms for enrollment, or non-secure portions of a financial transaction, and reconfiguration information for dialing and logging into the private portion of the transaction. The Bridging Software then hangs up the Internet connection, edits the user terminal's browser, stack and dialer files to reconfigure the terminal to connect to the private server. Prior to automatic redialing of the new private site for the user, the Bridging Software may be instructed by the application operating at WWW Server Node 330 to display items chosen for purchase, or to display a form for the end-user to complete off-line before dialing the private application. Upon connecting to the private application and completing the transaction as to the user sensitive information in a private environment, the Bridging Software then restores the end-user software to the dialing and authorization parameters required to dial to the public Internet.

A particularly advantageous application of the automated reconfiguration and information transfer methodology of the Bridging Software is that it adds value to certain WWW servers which do not possess the Common Gateway Interface ("CGI") capability -- *i.e.*, a provision of specialized functions on the server beyond just displaying HTML files, and are accordingly unable to accomplish any transactional processing in respect to items selected by a user. In effect, such a non-CGI server, on its own, can only serve as a "billboard" for the items represented in its database.

However, with the collection and redelivery process of the Bridging Software, a data capture and processing mechanism can be implemented for servers operating in a non-CGI environment -- such servers being incapable of more than the simple delivery of static data packets corresponding to available items. The data set enabled by the Bridging Software is a mechanism for augmenting such limited server capabilities by defining a flexible mechanism for the receipt, display, and delivery of arbitrary data from one site to another.

In such a scenario, the Bridging Software receives a "shopping cart" item list from the host as a data-set defined with a static MIME data packet associated with the Bridging Software. This information comprising the data-set may be updated, displayed to the user in a "read-only" fashion, or presented to the user for order selection.

During the process of interacting with the WWW server, a user may trigger HTML links resulting in additional MIME packets for the Bridging Software being delivered to the client. These packets allow items to be added and/or removed from the specified data set or presented to the user for local confirmation. The user will interact with a pop-up screen provided by the Bridging Software which presents the items available with product information, such as part number, description, unit cost, etc. The user identifies those items which are to be placed into the "shopping cart" and the quantity of items desired. Upon completion of the form, the Bridging Software stores the order in a format suitable for subsequent delivery to the private server site.

An additional feature provided by the methodology of the Bridging Software is an automated mechanism for providing compatibility with user terminals not previously having the Bridging Software included with the terminal's browser. To that end, the Bridging Software located at an accessed public network site initially checks to see if the browser counterpart for that software is loaded at the calling user terminal. If yes, the heretofore described processes of the Bridging Software go forward. If not however, a request is sent through the public host to download the Bridging Software to the calling terminal. After such a download, a helper application loads the Bridging Software to the terminal's browser.

I. Illustrative Embodiments

A variety of browser reconfiguration applications are supported by the automated browser reconfiguration means of the invention. Four essentially diverse capabilities of this invention, which support such applications, are described hereafter as illustrative embodiments of the invention.

A. Basic Jump Capabilities

In this configuration, which is illustrated in flow chart form in Figure 4, an end-user is connected to a chosen WWW serving node (where a desired information product is made available) via a modem and an Internet browser associated with the user's terminal (Step 401 of Figure 4). After conducting an information transaction with the selected WWW serving node for some interval (determined in relation to the specific application accessed), the user clicks on a hyper-text link, or picture, to begin an automated process which will cause that public session to be terminated and a new connection established to an alternate private data network (Step 402).

In response to that user action, a data message containing parameter reconfiguration instructions is passed from the WWW server application to the Bridging Software at the user's terminal (Step 403). Upon receiving such instructions, the Bridging Software edits the user's on-line communications software parameters, reconfiguring that software to dial the alternate data network (Step 404). This reconfiguration is fully automatic and transparent to the user, and includes parameters such as modem dial number, login, password, and TCP/IP addresses. At that point, the Bridging Software causes the modem to disconnect the current data network connection, shutting down the browser, and to then dial the alternate private data network (Step 405).

With the establishment of a connection to the private server on the alternate data network, the user interacts with the alternate data network application as appropriate (Step 406), and after an interval completes his activity with the alternate data network and provides an indication of such completion (Step 407). A data message containing parameter reconfiguration instructions is then passed from the alternate data network application to the Bridging Software (Step 408).

At that point, the Bridging Software again edits the user's on-line communications software parameters, reconfiguring them to dial the original public data network, or another preselected network (Step 409). As with the first reconfiguration, this configuration is automatic and includes parameters such as modem dial number, login, password, and TCP/IP addresses. The Bridging Software automatically causes the current private data network to be disconnected by the modem (Step 410), and if appropriate, causes the original public data network to be redialed (Step 411). When such a reconnection to the public data network is established, the end-user would then continue his application in the public data network.

B. "Shopping Cart" Capability

With this configuration, illustrated in flow chart form in Figure 5, a user begins by establishing a connection to a WWW application (assuming for the moment that the application is non-CGI enabled) at a serving node for that application, using the Internet browser and modem associated with the user's terminal (Step 501 of Figure 5). Upon finding an item in that application to be saved, or remembered for later consideration, or purchase, the user clicks on a hyper-text link, or picture, representing that item (Step 502). That application then sends a data message to the Bridging Software containing information about the items selected (Step 503) and such information is stored by the Bridging Software.

ware in the "shopping cart" file in the user's terminal (**Step 504**). Such selection download and storage steps (*i.e.*, steps 502, 503 & 504) are repeated for as many items as the user chooses to select. At any point after the Bridging Software has received the first set of item selection information, the user can instruct the Bridging Software to cause those selected items about which such information has been received to be displayed locally (at the user's terminal), where the user may review or edit (including deletion if desired) the collection of items theretofore selected. The application may also control display characteristics such as color and font for such locally displayed items. Note that in the case of a CGI-enabled application, the application itself will keep track of the items selected by the user and only download the totality of the selected items at the end of the selection process, and accordingly, the described local display option will not be applicable to such a CGI-enabled application.

At the point of completion of his "shopping", the user clicks on a hyper-text link or picture to "check out" (**Step 505**), which will begin a process of causing a jump to an alternate data network for the completion of sensitive portions of the transaction. To that end, a data message containing parameter reconfiguration instructions is passed from the WWW application to the Bridging Software (**Step 506**). It is to be noted that, as a security measure, information such as the new dial number, IP address, home page, configuration data (*e.g.*, login, password, DNS address) may be passed over the public network in encrypted form.

Upon receiving such reconfiguration instructions, the Bridging Software edits the user's on-line communications software parameters, reconfiguring that software to dial the alternate data network (**Step 507**). This reconfiguration is fully automatic and transparent to the user, and includes parameters such as modem dial number, login, password, and TCP/IP addresses. At that point, the Bridging Software causes the modem to disconnect the current data network connection, shutting down the browser, and to then dial the alternate data network (**Step 508**).

The Bridging Software passes the stored "shopping cart" data captured from the WWW application to the alternate network application (**Step 509**), where that data may be displayed for the user, permitting the user to confirm and/or modify the data (**Step 510**). The user interacts with the alternate data network application as appropriate, and after an interval completes his activity with the alternate data network (**Step 511**) and thus, by providing an appropriate completion signal to the application, completing the private portion of the information transaction (**Step 512**). A data message containing parameter reconfiguration instructions is then passed from the alternate data network application to the Bridging Software (**Step 513**).

The Bridging Software, at this point, again edits the user's on-line communications software parameters, reconfiguring them to dial the original (or another pre-defined) data network (**Step 514**). As with the first reconfiguration, this configuration is automatic and includes parameters such as modem dial number, login, password, and TCP/IP addresses. The Bridging Software automatically causes the current private data network to be disconnected by the modem (**Step 515**), and if appropriate, causes the original public data network to be redialed (**Step 516**). When such a reconnection is established to the point in the public data network where the user had left off to handle the secured aspects of his information transaction, the user would then continue his application in the public data network.

C. Stored Configuration Capabilities

For this configuration, depicted in flow chart form in Figure 6, an end-user is connected to a chosen WWW serving node (where a desired information product is made available) via a modem and an Internet browser associated with the user's terminal (**Step 601** of Figure 6). The user selects a hypertext link or picture associated with the WWW application by clicking on such link or picture (**Step 602**). A data message containing parameter reconfiguration instructions and an application icon (related to the selected hypertext link or picture) is passed from the WWW application to the Bridging Software (**Step 603**).

The Bridging Software creates an icon for display at the user's terminal, and saves a Bridging Software configuration file that is associated with that icon (**Step 604**). Such Bridging Software actions are automatic and multiple selections may be captured in this manner. At this point the user may continue the on-line session, or, if all desired selections have been made, a signal is provided from the user that the session should be discontinued (**Step 605**). The Bridging Software then automatically disconnects the current data network connection (**Step 606**).

After disconnecting from the WWW application, and following an interval determined by the user, a new application is selected by the user by clicking on the appropriate new icon displayed at the user's terminal (**Step 607**). The Bridging Software receives the reconfiguration instructions from the file associated with the selected icon (**Step 608**).

The Bridging Software edits the user's on-line communications software parameters, reconfiguring that software to dial the alternate data network (**Step 609**). The Bridging Software then automatically starts the user's Internet browser software and causes the alternate network application to be dialed by the modem associated with that terminal (**Step 610**). Upon establishing a connection to the alternate network, the user interacts with that application and completes the transaction to the user's satisfaction (**Step 611**). After a signal is sent to the alternate network indicating such completion of the user's activity (**Step 612**), a data message containing parameter reconfiguration instructions is passed from the alternate data network application to the Bridging Software (**Step 613**). That Software then causes the user's

terminal configuration parameters to be reset (**Step 614**) and the alternate data network to be automatically disconnected (**Step 615**).

D. Off-Line Form Capability

In this configuration, depicted in flow chart form in Figure 7, an end-user is connected to a chosen WWW serving node (where a desired information product is made available) via a modem and an Internet browser associated with the user's terminal (**Step 701** of Figure 7). The user selects a hypertext link or picture associated with an off-line form application -- an exemplary such form being an HTML-based form -- by clicking on such link or picture (**Step 702**). A data message containing parameter reconfiguration instructions for the Bridging Software, the selected off-line-form application, and an optional icon (related to the selected hypertext link or picture) is passed from the WWW application to the Bridging Software (**Step 703**). Note that the selected off-line form may be for either single or multiple use.

In the case of a delayed or multiple use of the selected form, the Bridging Software may create an icon for display at the user's terminal, and will save a Bridging Software configuration file that is associated with that icon (**Step 704**). The form in question is also saved on the user's terminal. Such Bridging Software actions are automatic. At this point the user may continue the on-line session, or, if all desired selections have been made, a signal is provided from the user that the session should be discontinued (**Step 705**). The Bridging Software then automatically disconnects the current data network connection (**Step 706**).

After disconnecting from the WWW application, two cases are to be considered as to the further processing of the selected form: (1) an immediate single use of the form and (2) either a delayed or multiple use of the form. In the first case, the Bridging Software edits the user's on-line communications software parameters, reconfiguring that software to dial the alternate data network. The Bridging Software then automatically starts the user's Internet browser software which is caused to display the off-line form. The user then completes the off-line form and chooses a "Submit Form" button displayed at his terminal.

In the second case, the Bridging Software will have created an icon for display at the user's terminal and saved a Bridging Software configuration file associated with that icon. Following an interval determined by the user, the off-line-form application is started by the user by clicking on the new form icon displayed at the user's terminal (**Step 707**). The Bridging Software receives the reconfiguration instructions from the file associated with the selected icon (**Step 708**).

The Bridging Software edits the user's on-line communications software parameters, reconfiguring that software to dial the alternate data network (**Step 709**). The Bridging Software then automatically starts the user's Internet browser software which is caused to display the off-line form (**Step 710**). The user then completes the off-line form and chooses a "Submit Form" button displayed at his terminal (**Step 711**).

In either the first or second case, following activation of the "Submit Form" button, the alternate network application is then caused to be dialed by the Bridging Software. Upon establishing a connection to the alternate network, the form data is passed to the alternate network (**Step 712**). The user then interacts with that application and completes the application (**Step 713**). After a signal is sent to the alternate network indicating such completion of the user's activity (**Step 714**), a data message containing parameter reconfiguration instructions is passed from the alternate data network application to the Bridging Software (**Step 715**). That Software then causes the user's terminal configuration parameters to be reset (**Step 716**) and the alternate data network to be automatically disconnected (**Step 717**).

CONCLUSION

A system and method has been described for the automatic switching of an information transaction between two or more alternate networks. This functionality, which incorporates a reconfiguration means designated herein as the Bridging Software, supports the movement of application specific data from one on-line environment to another. Among potential applications of this process for passing data between different environments are: selected items for purchase ("shopping cart"), captured data from forms, and other server captured data such as web pages visited.

The Bridging Software reconfiguration means is intended to work with various Web Browser software implementations, including the Netscape Personal Edition (NPE) Software for Windows 3.1 and 3.11, and which represents a working embodiment for the invention. The Bridging Software installs itself as a helper application within the browser application and utilizes a special MIME type configuration file to pass reconfiguration and "shopping cart" information from the server to the client software.

When an application requires a user to re-connect to a private application, a reconfiguration file is passed to the Bridging Software helper application via a CGI script or simple hyper-text link. The helper application disconnects the current data connection, reconfigures the dial parameters (dial #, login password, DNS address, and home page) and initiates the dial program so the end-user can access the private application.

When the end-user connects to the private application, the Bridging Software reconfiguration means provides the new "private server" application with data collected from the "public server", and the application resumes in a private,

secure environment.

The Bridging Software allows both short term and long term storage of dial configurations. Configurations passed to the Bridging Software can be designated as single use configurations and discarded after the application has terminated, or saved and displayed to the end-user as a dial choice by the Bridging Software.

5 Although the present embodiment of the invention has been described in detail, it should be understood that various changes, alterations and substitutions can be made therein without departing from the spirit and scope of the invention as defined by the appended claims. In particular, it is noted that, while the invention has been primarily described in terms of a preferred embodiment based on an automatic reconfiguration between a public and a private data network, any the methodology of the invention will be equally applicable to any set of alternate networks.

10

Claims

1. A method for managing a transaction via a communications path between a terminal device and a serving node in a data network, said method comprising the steps of:

15

establishing an initial communications path via a first connection between said terminal device and a serving node in a first data network;
receiving information from said serving node in said first data network for effecting a reconfiguration of said communications path for said transaction from said first connection in said first data network to a second connection in a second data network; and
20 automatically connecting said terminal device to a serving node in said second data network via said second connection.

20

2. A method for managing a transaction via a communications path between a terminal device and a serving node in a data network, said method comprising the steps of:

25

establishing an initial communications path via a first connection between said terminal device and a serving node in a first data network;
selecting at least one information item from a data base of said information items provided at said serving node in said first data network;
30 causing said selected information items to be downloaded to said terminal device via said first connection;
receiving information from said serving node in said first data network for effecting a reconfiguration of said communications path for said transaction from said first connection in said first data network to a second connection in a second data network; and
35 automatically connecting said terminal device to a serving node in said second data network via said second connection.

30

35

3. A method for managing a transaction via a communications path between a terminal device and a serving node in a data network, said method comprising the steps of:

40

establishing an initial communications path via a first connection between said terminal device and a serving node in a first data network;
identifying at least one data network application from a data base of said data network applications provided at said serving node in said first data network;
45 receiving information from said serving node in said first data network for reconfiguring said terminal device for implementation of a communication path via an alternate connection between said terminal device and at least one of said identified data network applications in a second data network; and
in response to a selection signal from a user, automatically connecting said terminal device to a selected one of said identified data network applications via said alternate connection.

50

4. A method for managing a transaction via a communications path between a terminal device and a serving node in a data network, said method comprising the steps of:

55

establishing an initial communications path via a first connection between said terminal device and a serving node in a first data network;
selecting an off-line form application from a data base provided at said serving node in said first data network;
receiving information from said serving node in said first data network for reconfiguring said terminal device for implementation of a communication path via a second connection between said terminal device and said

selected off-line form application in a second data network; and
in response to, a selection signal from a user, automatically connecting said terminal device to said selected off-line form application.

- 5 5. The method for managing a transaction of Claim 1 or 2 including the further step of recognizing a signal to reconfigure said communications path from said first connection to said second connection.
6. The method for managing a transaction of Claim 3 wherein said selected data network application is operated at a serving node in said second data network.
- 10 7. The method for managing a transaction of Claim 4 wherein said selected off-line form application is operated at a serving node in said second data network.
8. The method for managing a transaction of one of the Claims 1, 2, 6 or 7 wherein said serving nodes in said first and said second data networks are manifested in a common node.
- 15 9. The method for managing a transaction of Claim 1 or 2 wherein said step of receiving information includes the further step of effecting said reconfiguration of said communications path.
- 20 10. The method for managing a transaction of Claim 1 or 2 wherein said step of automatically connecting includes the step of automatically disconnecting said first connection prior to implementation of said second connection.
11. The method for managing a transaction of Claim 1 or 2 including the further steps of:
- 25 automatically disconnecting said second connection in response to a user signal; and reconfiguring said terminal device to enable, in response to user instruction, an implementation of a connection via an identified data network.
12. The method for managing a transaction of Claim 11 wherein said step of automatically reconfiguring said terminal device includes the step of effecting said implementation of said connection via said identified data network.
- 30 13. The method for managing a transaction of Claim 2 wherein said step of causing said selected information items to be downloaded includes the further step of causing said selected information items to be displayed at said terminal device.
- 35 14. The method for managing a transaction of Claim 13 wherein said displayed selected items can be edited by a user at said terminal device.
15. The method for managing a transaction of Claim 13 wherein display characteristics for said displayed selected items can be controlled at said terminal device.
- 40 16. The method for managing a transaction of Claim 2 wherein said step of automatically connecting includes the step of uploading said selected information items from said terminal device to said service provider via said second connection.
- 45 17. The method for managing a transaction of Claim 3 including the further steps of:
- 50 automatically disconnecting said alternate connection in response to a user signal; and reconfiguring said terminal device to enable implementation of a pre-selected connection between said terminal device and an identified data network.
18. The method for managing a transaction of Claim 17 wherein said step of automatically reconfiguring said terminal device includes the further step of effecting said implementation of said pre-selected connection.
- 55 19. The method for managing a transaction of Claim 4 including the further step of downloading from said serving node in said first data network to said terminal device of an off-line form related to said off-line form application.
20. The method for managing a transaction of Claim 4 including the further step of uploading said downloaded off-line

form from said terminal device to said selected off-line form application, after processing by a user.

21. The method for managing a transaction of Claim 4 including the further steps of:

5 automatically disconnecting said connection to said selected off-line form application in response to a user signal; and
reconfiguring said terminal device to enable implementation of a pre-selected connection between said terminal device and an identified data network.

10 22. The method for managing a transaction of Claim 21 wherein said step of automatically reconfiguring said terminal device includes the further step of effecting said implementation of said pre-selected connection.

23. A method for managing connections between a terminal device and at least one information source/processor wherein at least two of said connections are implemented via separate communications networks, comprising the steps of:

15 recognizing a signal for connection to an information source/processor via a communications network other than a communications network for which a predetermined connection is configured;
causing said terminal device to implement a connection to said information source/processor via said other communications network; and
20 upon termination of said information source/processor connection via said other communications network, automatically reconfiguring a connection criteria in said terminal device to enable said terminal device to implement, in response to user instruction, a connection via an alternative one of said communications networks.

25 24. The method for managing connections of Claim 23 wherein said recognizing step occurs at a point when said terminal device is connected to a given source/processor.

25. The method for managing connections of Claim 23 wherein information items may be selected by a user at said terminal device from said given source/processor, and including the further step of causing said selected information items to be downloaded from said source/processor to said terminal device.

30 26. The method for managing connections of Claim 25 wherein said step of effecting connection includes the further step of uploading said selected information items from said terminal device to said other information source/processor.

35 27. The method for managing connections of Claim 26 wherein said selected information items are processed by said user at said terminal device prior to uploading to said other information source/processor.

40 28. The method for managing connections of Claim 24 including the further step of causing said given source/processor to download to said terminal device configuration data for enabling said step of effecting connection to said other information source/processor.

45 29. The method for managing connections of Claim 24 including the further step of causing said other source/processor to download to said terminal device configuration data for enabling said step of automatically restoring a prior connection criteria in said terminal device.

30. A method for enhancing security of certain data in an on-line information transaction comprising the steps of:

50 bifurcating said information transaction into a first portion comprising said certain data and a remaining portion, wherein said remaining portion is carried out via a public on-line communications connection between a terminal device and a public information server;
causing said first portion to be carried out via a secure private on-line communications connection between said terminal device and a private information server; and
55 automatically reconfiguring network access means in said terminal device to switch between said public connection and said private connection.

FIG. 1

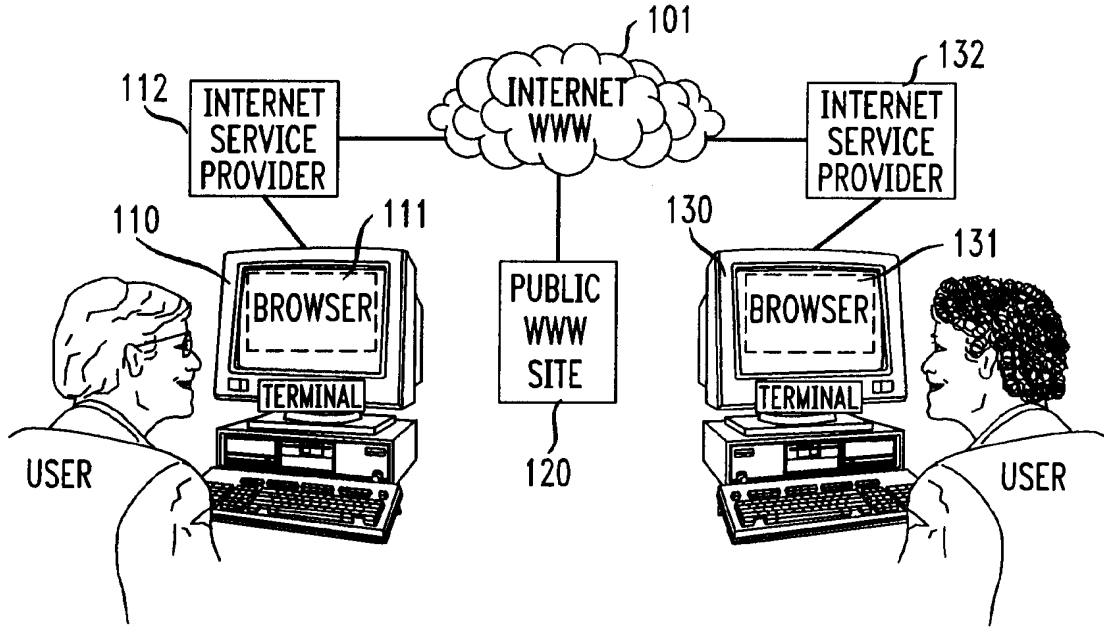


FIG. 2

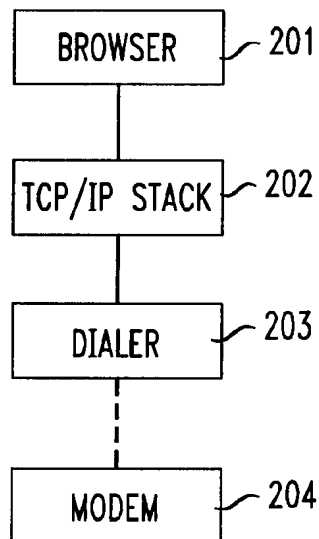


FIG. 3

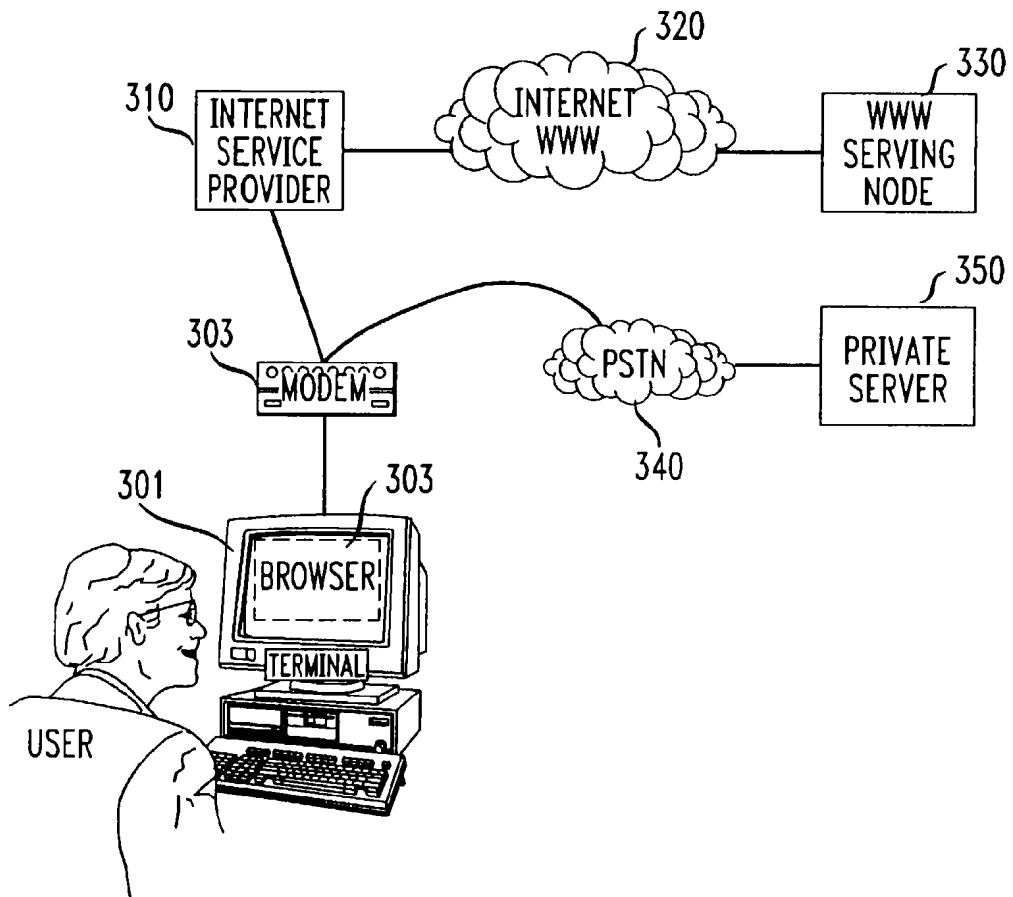


FIG. 4

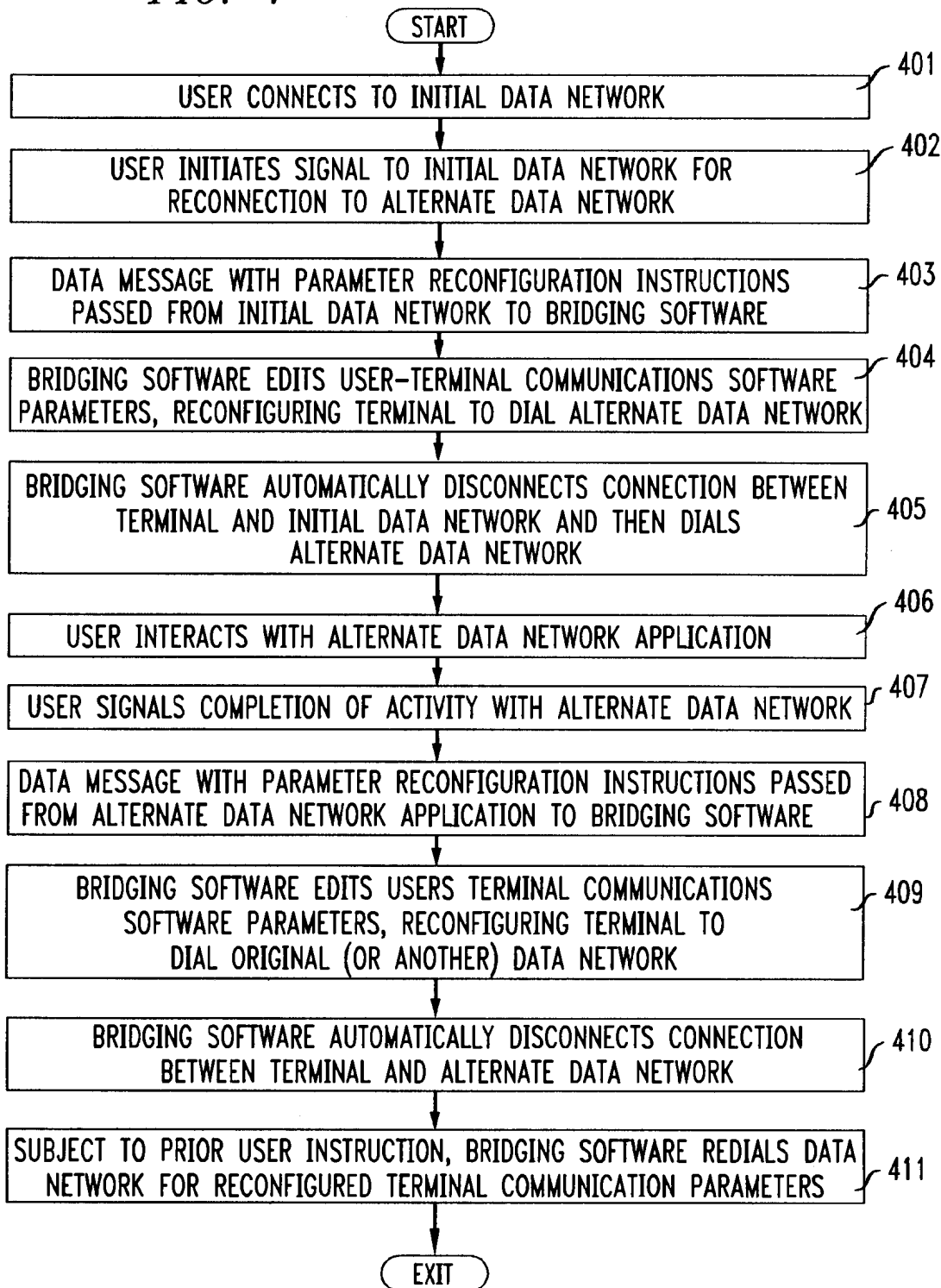


FIG. 5A

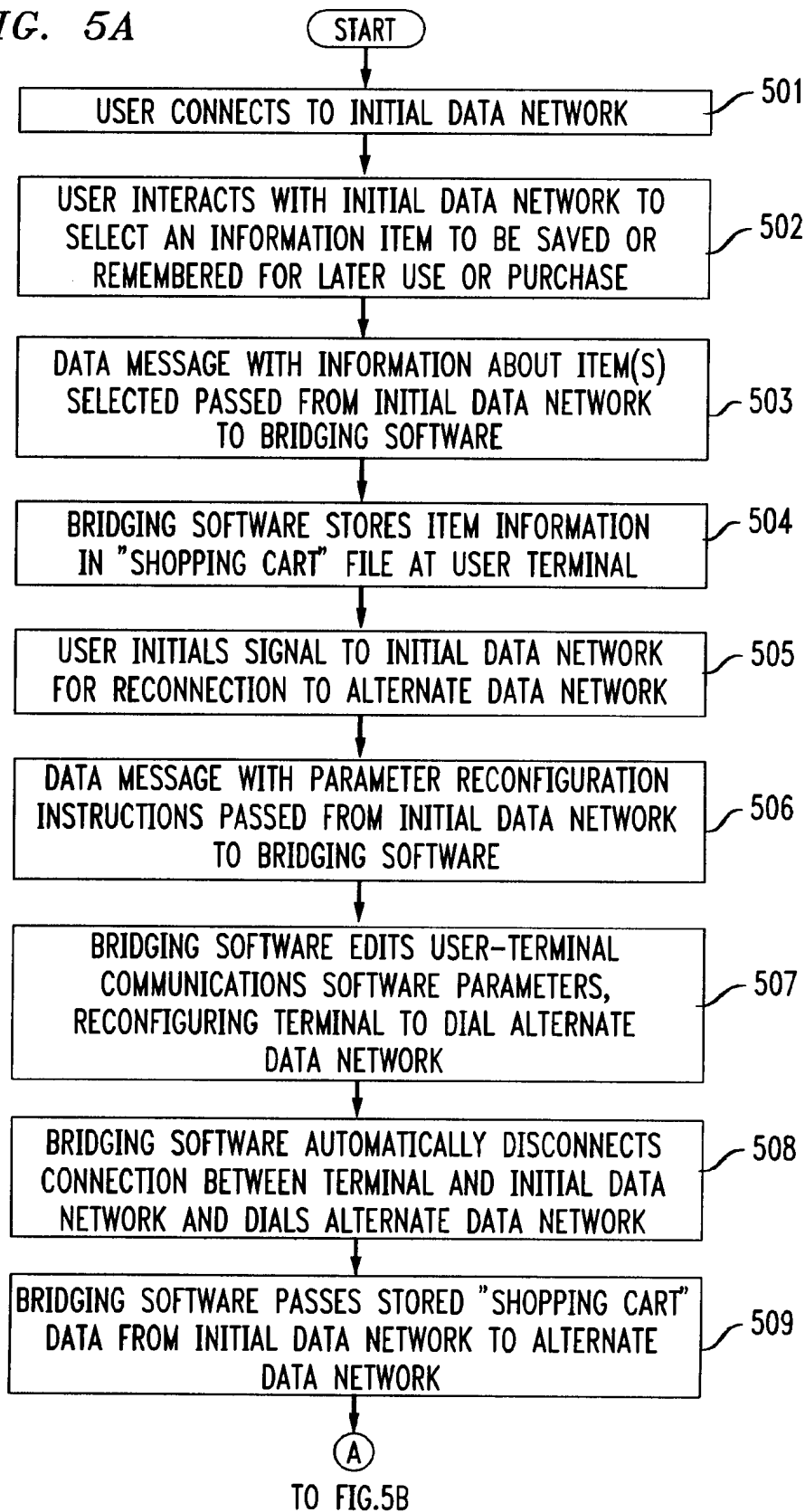


FIG. 5B

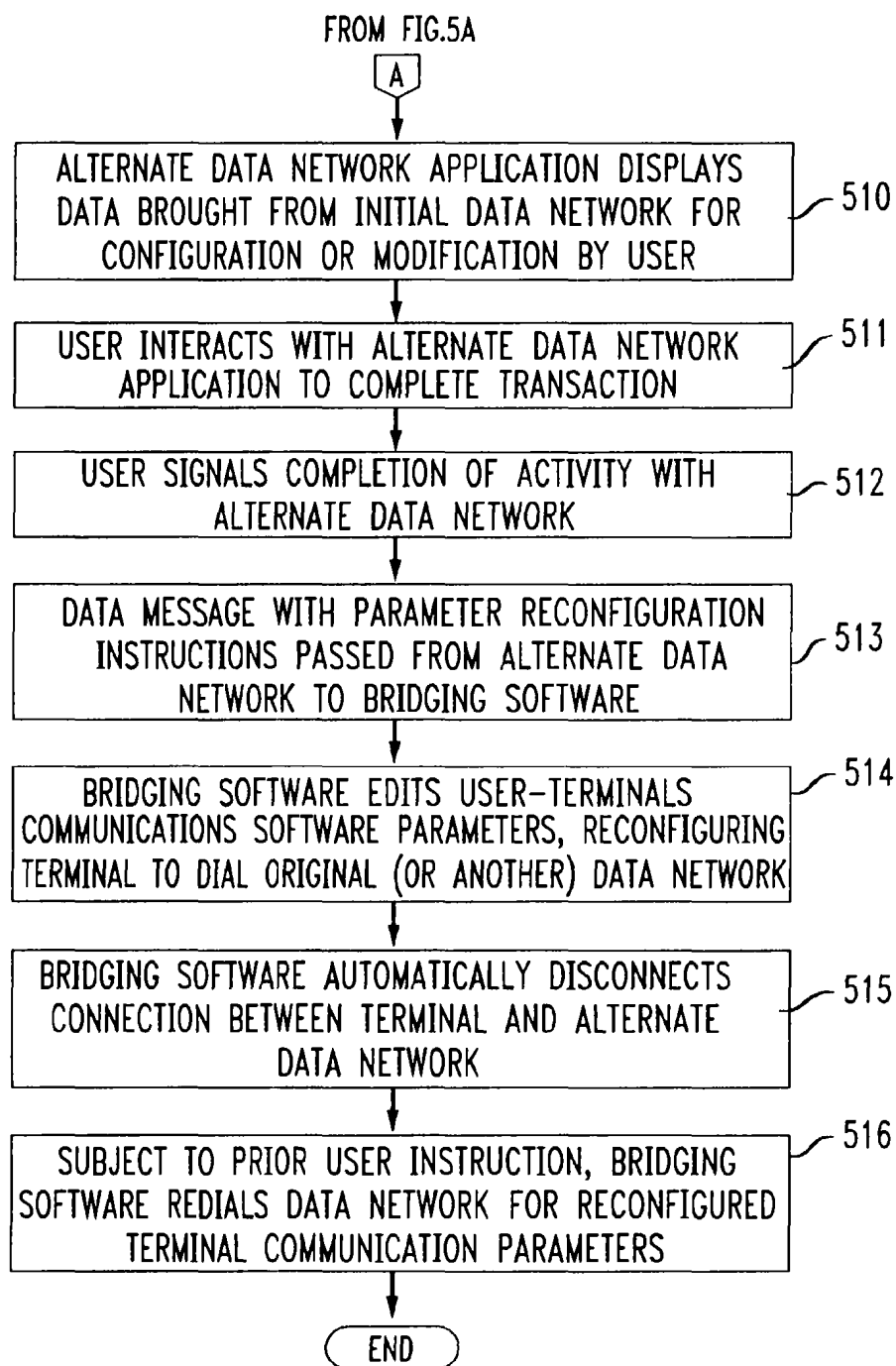


FIG. 6A

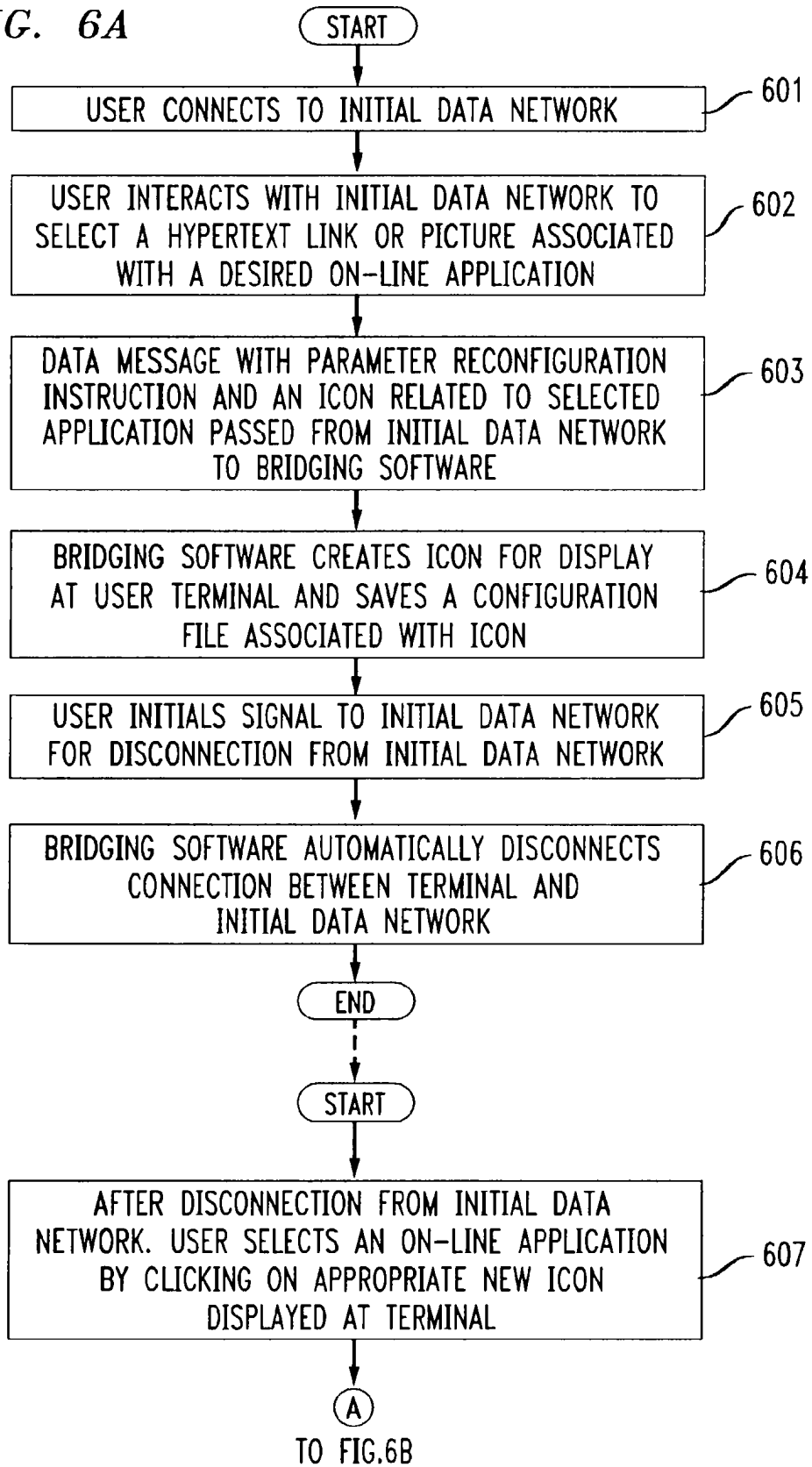


FIG. 6B

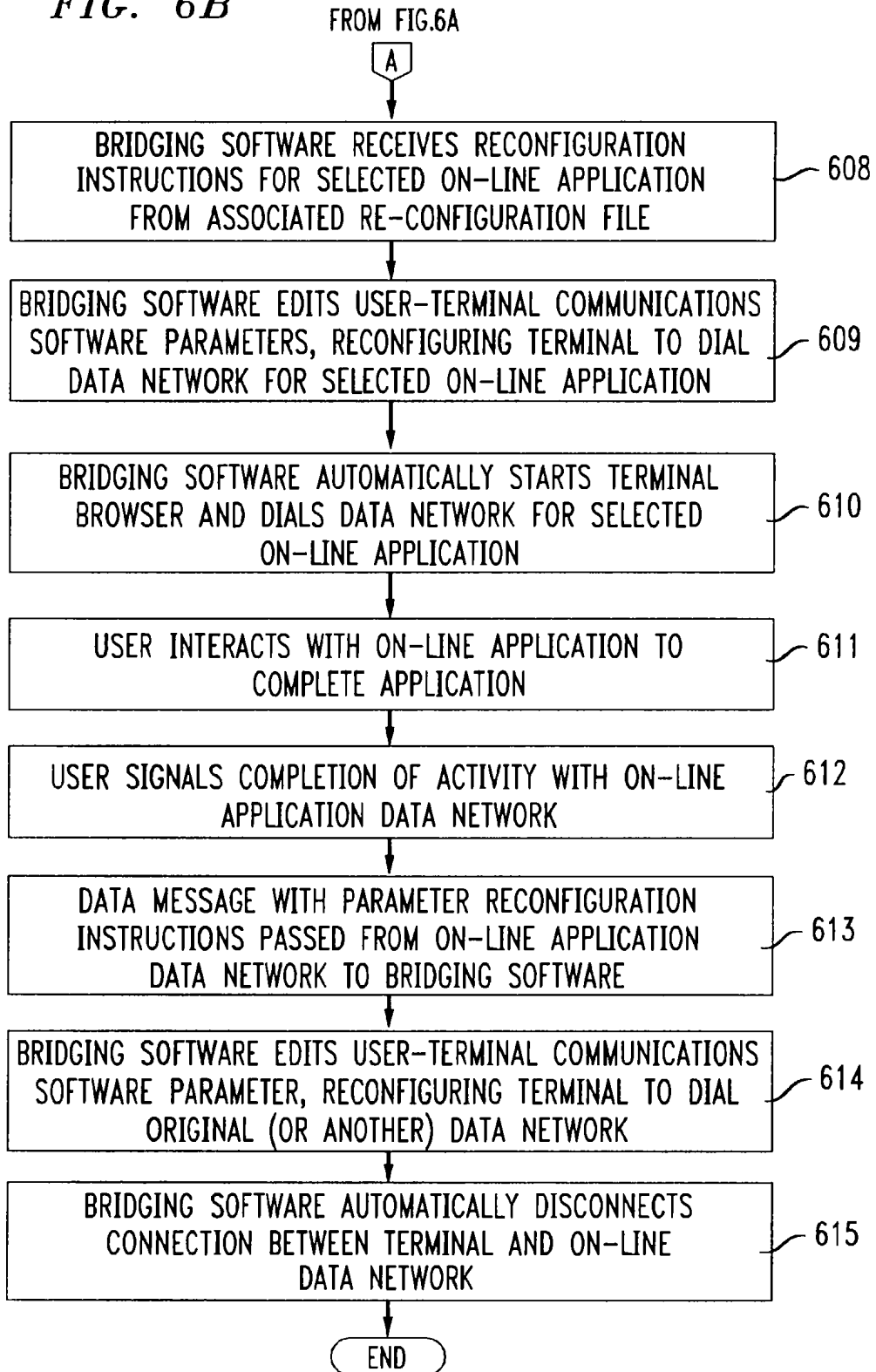


FIG. 7A

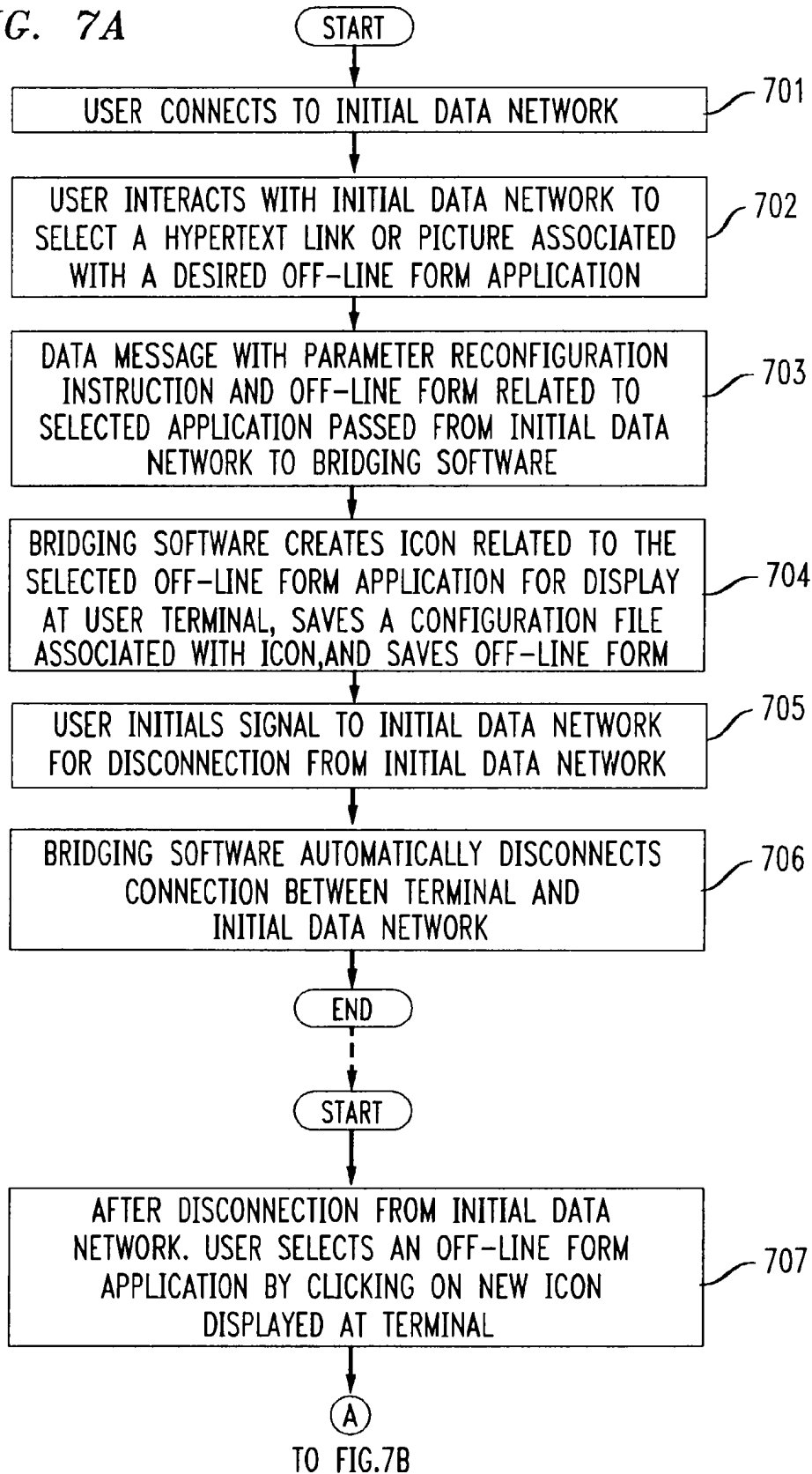
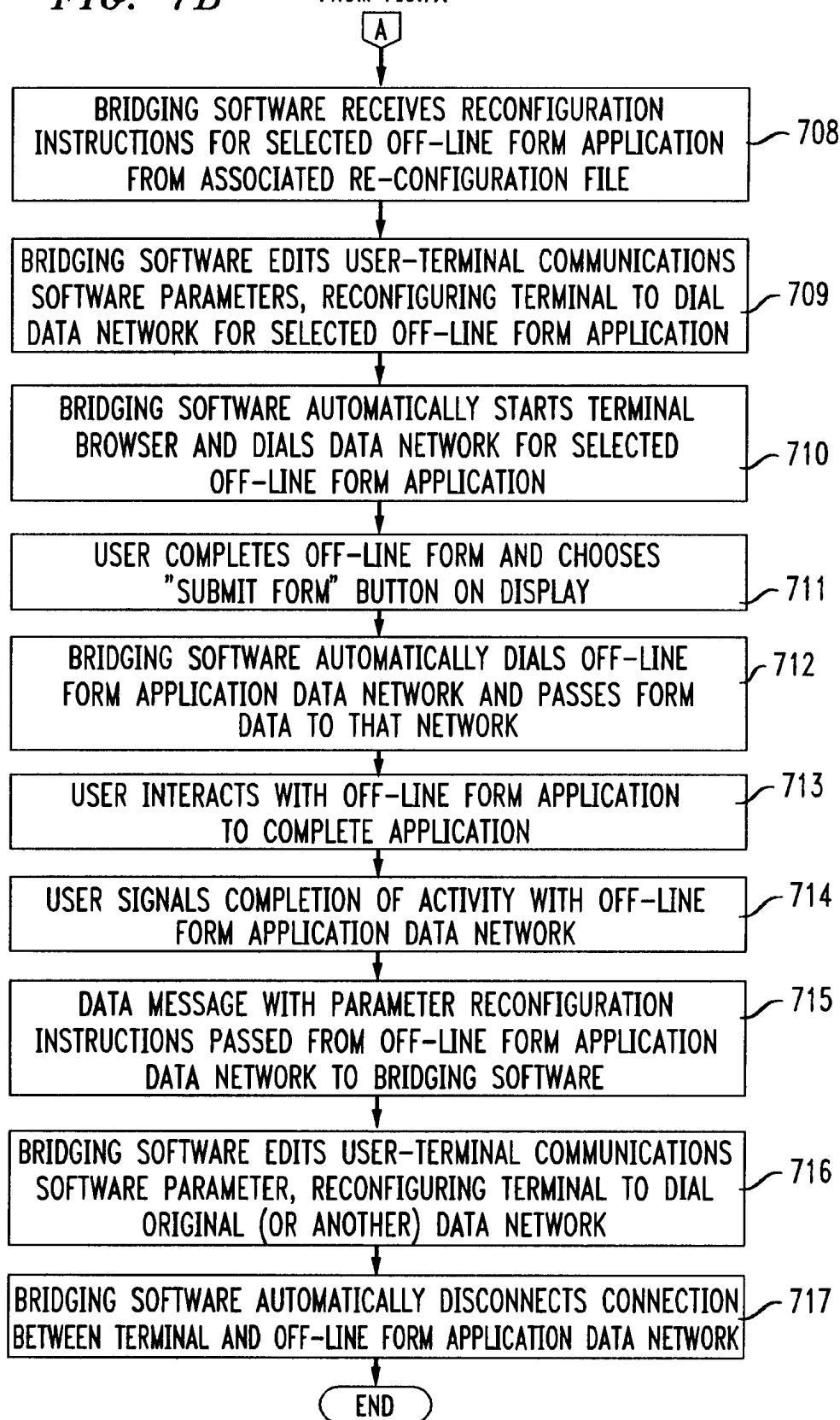


FIG. 7B

FROM FIG.7A



(12) **UK Patent Application** (19) **GB** (11) **2 317 792** (13) **A**

(43) Date of A Publication **01.04.1998**

(21) Application No **9719816.2**

(22) Date of Filing **17.09.1997**

(30) Priority Data

(31) **08715343** (32) **18.09.1996** (33) **US**
08715668 **18.09.1996**

(71) Applicant(s)

Secure Computing Corporation

(Incorporated in USA - Delaware)

**2675 Long Lake Road, Roseville,
Minnesota 55113-2536, United States of America**

(72) Inventor(s)

**Spence Minear
Edward B Stockwell
Troy De Jongh**

(74) Agent and/or Address for Service

**Beresford & Co
2-5 Warwick Court, High Holborn, LONDON,
WC1R 5DJ, United Kingdom**

(51) INT CL⁶
H04L 9/00

(52) UK CL (Edition P)
**H4P PPEB
U1S S2124 S2209**

(56) Documents Cited

**WO 97/26735 A1 WO 97/26734 A1 WO 97/26731 A1
WO 97/23972 A1 WO 97/13340 A1**

(58) Field of Search

**UK CL (Edition P) H4P PDCSA PDCSC PPEB
INT CL⁶ H04L 9/00 9/32 29/06 29/08
Online: WPI, INSPEC**

(54) **Virtual Private Network for encrypted firewall**

(57) A system (10) for regulating the flow of messages through a firewall (18) having a network protocol stack, wherein the network protocol stack includes an Internet Protocol (IP) layer where if the message is not encrypted, it passes the unencrypted message up the network protocol stack to an application level proxy (50), and if the message is encrypted, it decrypts the message and passes the decrypted message up the network protocol stack to the application level proxy. The step of decrypting the message includes the step of executing a process at the IP layer to decrypt the message.

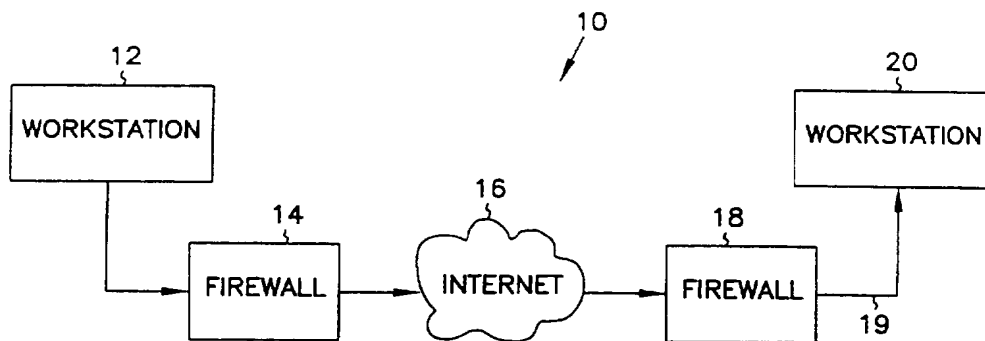


FIG. 1

GB 2 317 792 A

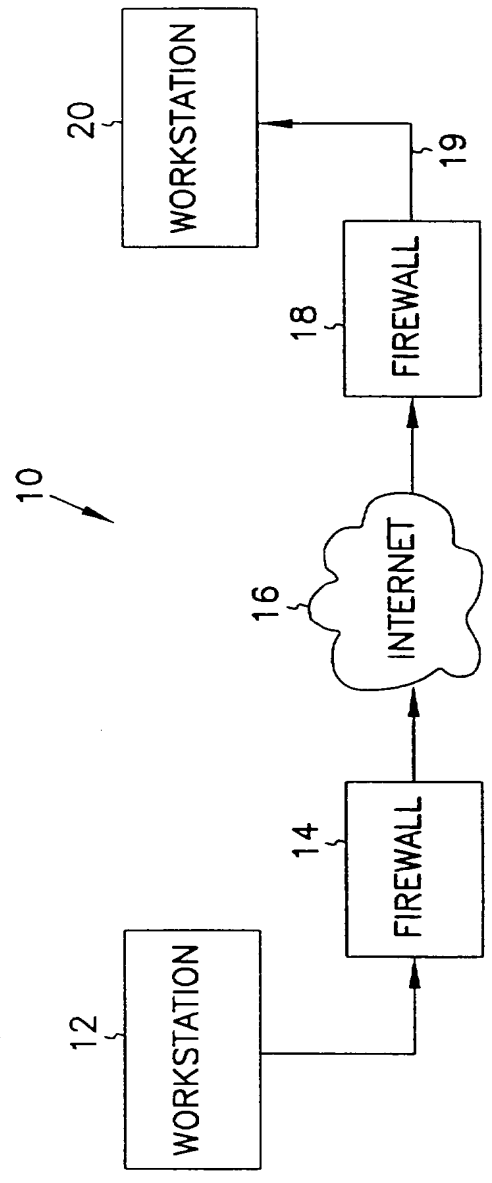


FIG. 1

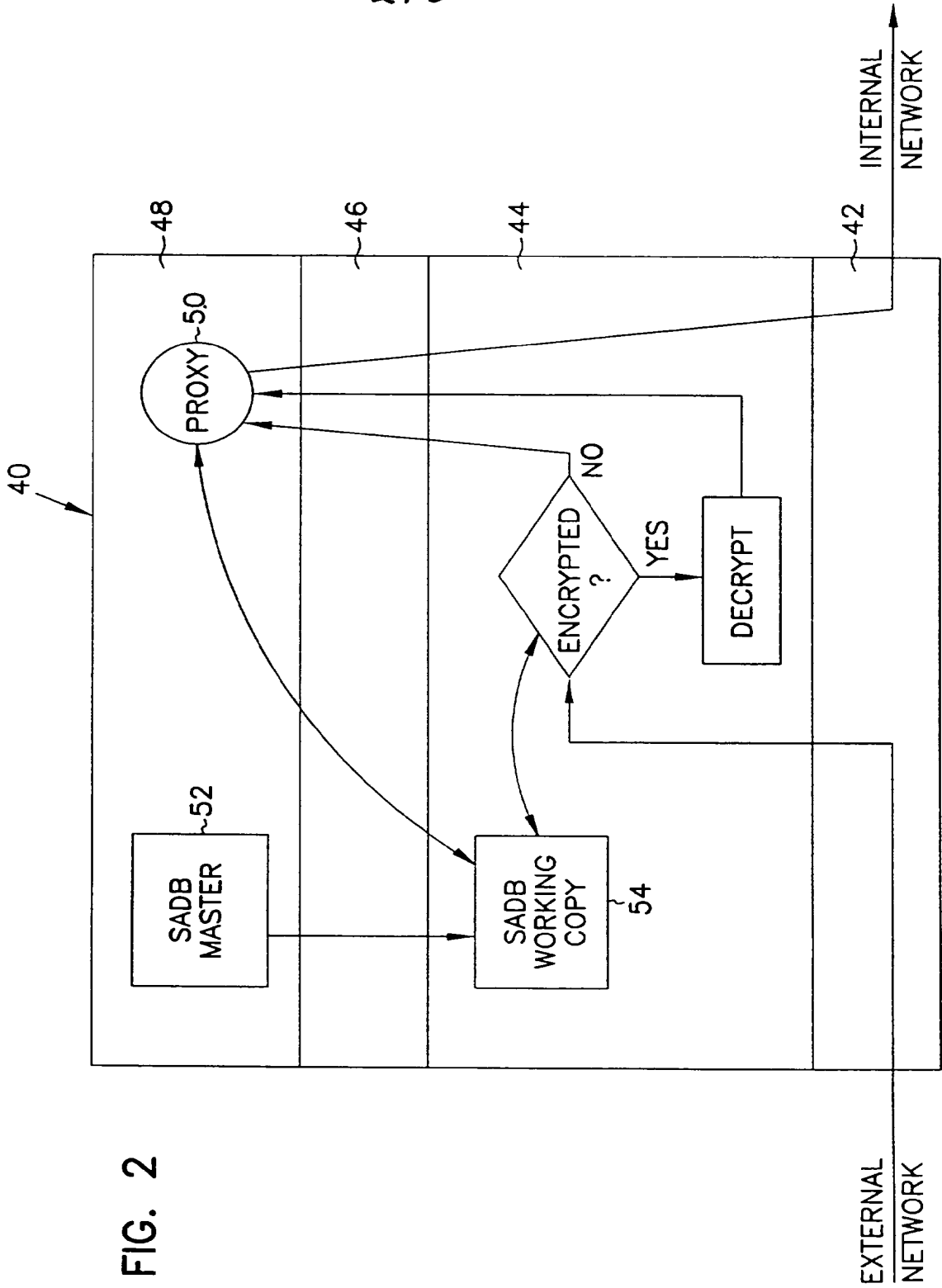
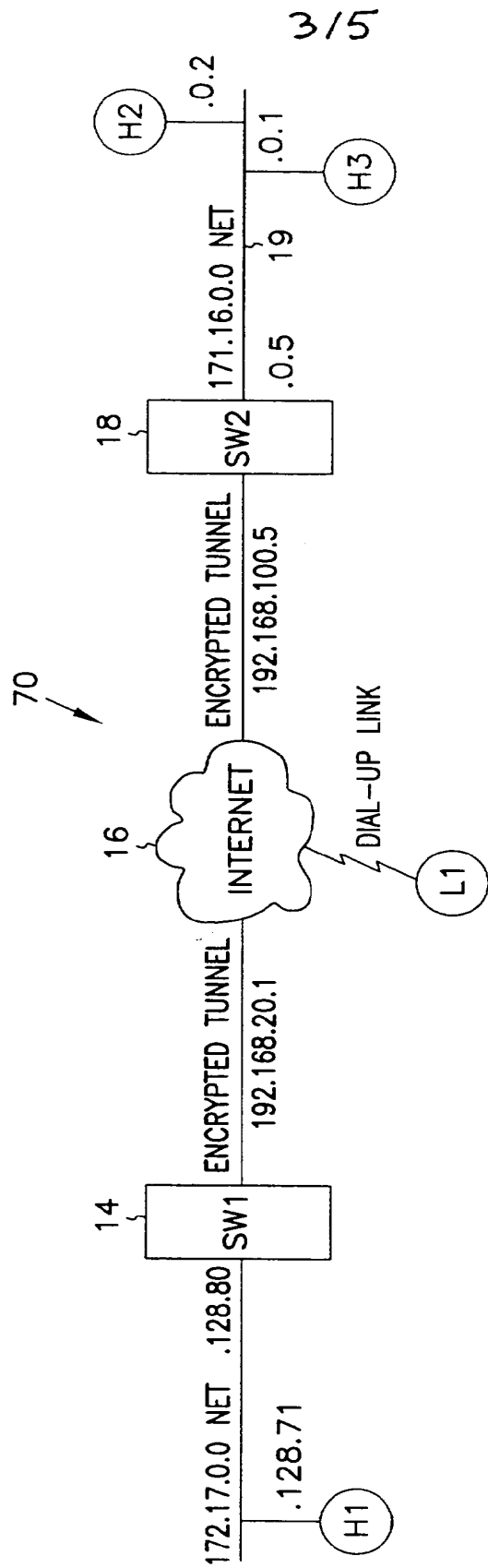


FIG. 2



3/5

FIG. 3

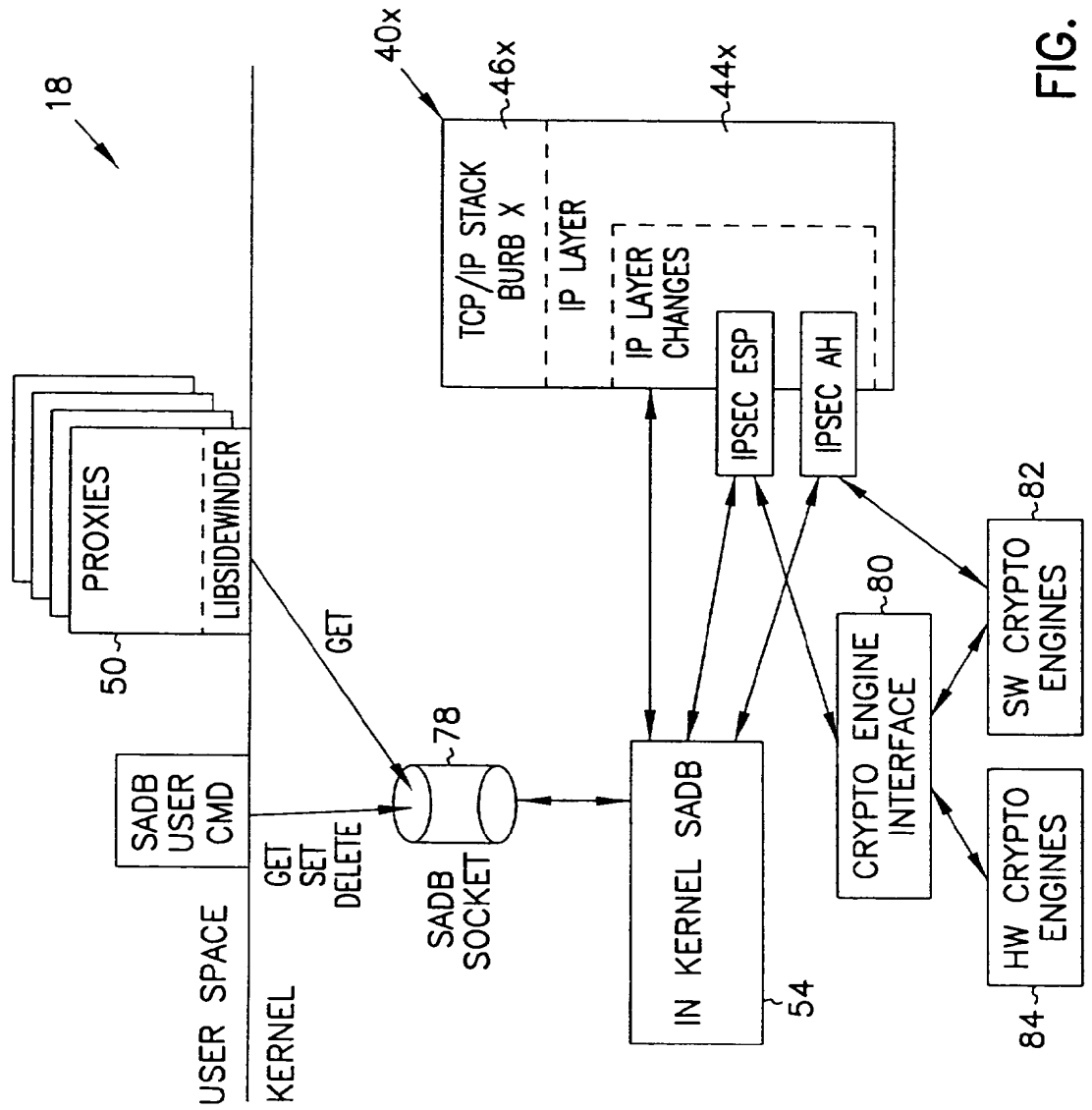


FIG. 4

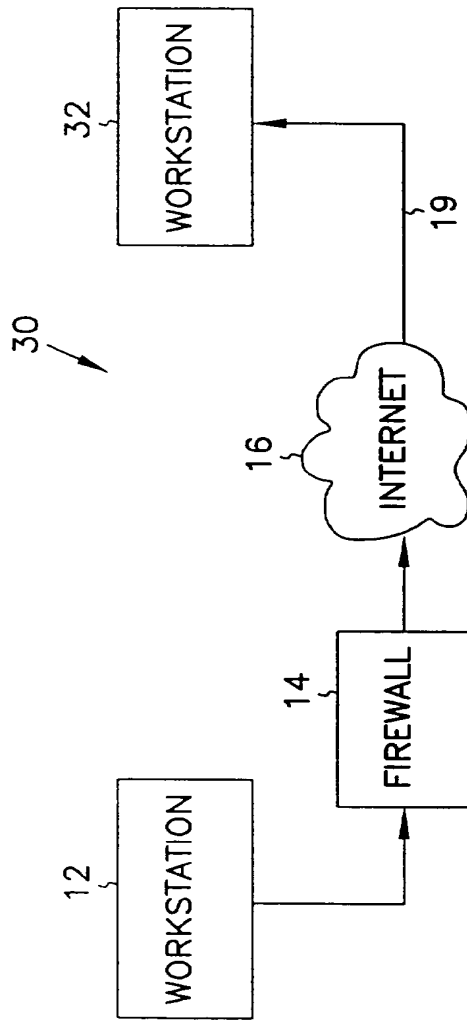


FIG. 5

VIRTUAL PRIVATE NETWORK ON APPLICATION GATEWAY

5 Background of the InventionField of the Invention

The present invention pertains generally to network communications, and in particular to a system and method for securely transferring information between firewalls over an unprotected network.

10 Background Information

Firewalls have become an increasingly important part of network design. Firewalls provide protection of valuable resources on a private network while allowing communication and access with systems located on an unprotected network such as the Internet. In addition, they operate to block attacks on a private network arriving from the unprotected network by providing a single connection with limited services. A well designed firewall limits the security problems of an Internet connection to a single firewall computer system. This allows an organization to focus their network security efforts on the definition of the security policy enforced by the firewall. An example of a firewall is given in 20 "SYSTEM AND METHOD FOR PROVIDING SECURE INTERNETWORK SERVICES" by Boebert et al. (PCT Published Application No. WO 96/13113, published on May 2, 1996), the description of which is hereby incorporated by reference. Another description of a firewall is provided by Dan Thomsen in "Type Enforcement: the new security model", *Proceedings: Multimedia: Full-* 25 *Service Impact on Business, Education, and the Home*, SPIE Vol. 2617, p. 143, August 1996. Yet another such system is described in "SYSTEM AND METHOD FOR ACHIEVING NETWORK SEPARATION" by Gooderum et al. (PCT Published Application No. WO 97/29413, published on August 14, 1997), the description of which is hereby incorporated by reference. All the above 30 systems are examples of application level gateways. Application level gateways use proxies or other such mechanisms operating at the application layer to process traffic through the firewall. As such, they can review not only the

message traffic but also message content. In addition, they provide authentication and identification services, access control and auditing.

Data to be transferred on unprotected networks like the Internet is susceptible to electronic eavesdropping and accidental (or deliberate) corruption.

5 Although a firewall can protect data within a private network from attacks launched from the unprotected network, even that data is vulnerable to both eavesdropping and corruption when transferred from the private network to an external machine. To address this danger, the Internet Engineering Task Force (IETF) developed a standard for protecting data transferred between firewalls
10 over an unprotected network. The Internet Protocol Security (IPSEC) standard calls for encrypting data before it leaves the first firewall, and then decrypting the data when it is received by the second firewall. The decrypted data is then delivered to its destination, usually a user workstation connected to the second firewall. For this reason IPSEC encryption is sometimes called *firewall-to-*
15 *firewall encryption* (FFE) and the connection between a workstation connected to the first firewall and a client or server connected to the second firewall is termed a *virtual private network*, or VPN.

The two main components of IPSEC security are data encryption and sender authentication. Data encryption increases the cost and time required for
20 the eavesdropping party to read the transmitted data. Sender authentication ensures that the destination system can verify whether or not the encrypted data was actually sent from the workstation that it was supposed to be sent from. The IPSEC standard defines an encapsulated payload (ESP) as the mechanism used to transfer encrypted data. The standard defines an authentication header (AH)
25 as the mechanism for establishing the sending workstation's identity.

Through the proper use of encryption, the problems of eavesdropping and corruption can be avoided; in effect, a protected connection is established from the internal network connected to one firewall through to an internal network connected to the second firewall. In addition, IPSEC can be used to provide a
30 protected connection to an external computing system such as a portable personal computer.

IPSEC encryption and decryption work within the IP layer of the network protocol stack. This means that all communication between two IP addresses will be protected because all interfirewall communication must go through the IP layer. Such an approach is preferable over encryption and decryption at higher levels in the network protocol stack since when encryption is performed at layers higher than the IP layer more work is required to ensure that all supported communication is properly protected. In addition, since IPSEC encryption is handled below the Transport layer, IPSEC can encrypt data sent by any application. IPSEC therefore becomes a transparent add-on to such protocols as TCP and UDP.

Since, however, IPSEC decryption occurs at the IP layer, it can be difficult to port IPSEC to an application level gateway while still maintaining control at the proxy over authentication, message content, access control and auditing. Although the IPSEC specification in RFC 1825 suggests the use of a mandatory access control mechanism in a multi-level secure (MLS) network to compare a security level associated with the message with the security level of the receiving process, such an approach provides only limited utility in an application level gateway environment. In fact, implementations on application level gateways to date have simply relied on the fact that the message was IPSEC-encrypted as assurance that the message is legitimate and have simply decoded and forwarded the message to its destination. This creates, however, a potential chink in the firewall by assuming that the encrypted communication has access to all services.

What is needed is a method of handling IPSEC messages within an application level gateway which overcomes the above deficiencies. The method should allow control over access by an IPSEC connection to individual services within the internal network.

Summary of the Invention

The present invention is a system and method for regulating the flow of messages through a firewall having a network protocol stack, wherein the network protocol stack includes an Internet Protocol (IP) layer, the method

comprising the steps of determining, at the IP layer, if a message is encrypted, if the message is not encrypted, passing the unencrypted message up the network protocol stack to an application level proxy, and if the message is encrypted, decrypting the message and passing the decrypted message up the network
5 protocol stack to the application level proxy, wherein the step of decrypting the message includes the step of executing a procedure at the IP layer to decrypt the message.

According to another aspect of the present invention, a system and method is described for authenticating the sender of a message within a
10 computer system having a network protocol stack, wherein the network protocol stack includes an Internet Protocol (IP) layer, the method comprising the steps of determining, at the IP layer, if the message is encrypted, if the message is encrypted, decrypting the message, wherein the step of decrypting the message includes the step of executing a procedure at the IP layer to decrypt the message,
15 passing the decrypted message up the network protocol stack to an application level proxy, determining an authentication protocol appropriate for the message, and executing the authentication protocol to authenticate the sender of the message.

Brief Description of the Drawings

20 In the following detailed description of example embodiments of the invention, reference is made to the accompanying drawings which form a part hereof, and which is shown by way of illustration only, specific embodiments in which the invention may be practiced. It is to be understood that other embodiments may be utilized and structural changes may be made without
25 departing from the scope of the present invention.

In the drawings, where like numerals refer to like components throughout the several views:

Figure 1 is a functional block diagram of an application level gateway-
30 implemented firewall-to-firewall encryption scheme according to the present invention;

Figure 2 is a block diagram showing access control checking of both encrypted and unencrypted messages in network protocol stack according to the present invention;

Figure 3 is a block diagram of a representative application level gateway-
5 implemented firewall-to-firewall encryption scheme;

Figure 4 is a block diagram of one embodiment of a network-separated protocol stack implementing IPSEC according to the present invention; and

Figure 5 is a functional block diagram of a firewall-to-workstation encryption scheme according to the present invention.

10

Description of the Preferred Embodiments

In the following detailed description of the preferred embodiment, references made to the accompanying drawings which form a part hereof, and in which is shown by way of illustration specific preferred embodiments in which
15 the invention may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention, and it is to be understood that other embodiments may be utilized and that structural, logical, physical, architectural, and electrical changes may be made without departing from the spirit and scope of the present invention. The following detailed
20 description is, therefore, not to be taken in a limiting sense, and the scope of the present invention is defined only by the appended claims and their equivalents.

A system 10 which can be used for firewall-to-firewall encryption (FFE) is shown in Figure 1. In Figure 1, system 10 includes a workstation 12 communicating through a firewall 14 to an unprotected network 16 such as the
25 Internet. System 10 also includes a workstation 20 communicating through a firewall 18 to unprotected network 16. In one embodiment, firewall 18 is an application level gateway.

As noted above, IPSEC encryption and decryption work within the IP layer of the network protocol stack. This means that all communications
30 between two IP addresses will be protected because all interfirewall communication must pass through the IP layer. IPSEC takes the standard

Internet packet and converts it into a carrier packet. The carrier packet is designed to do two things: to conceal the contents of the original packet (encryption) and to provide a mechanism by which the receiving firewall can verify the source of the packet (authentication). In one embodiment of the present invention, each IPSEC carrier packet includes both an authentication header used to authenticate the sending machine and an encapsulated payload containing encrypted data. The authentication header and the encapsulated payload features of IPSEC can, however, be used independently. As required in RFC 1825, DES-CBC is provided for use in encrypting the encapsulated payload while the authentication header uses keyed MD5.

To use IPSEC, you must create a *security association* (SA) for each destination IP address. In one embodiment, each SA contains the following information:

- Security Parameters Index (SPI) - The index used to find a SA on receipt of an IPSEC datagram.
- Destination IP address - The address used to find the SA and trigger use of IPSEC processing on output.
- The peer SPI - The SPI value to put on a IPSEC datagram on output.
- The peer IP address - The destination IP address to be put into the packet header if IPSEC Tunnel mode is used.
- The Encryption Security Payload (ESP) algorithm to be used.
- The ESP key to used for decryption of input datagrams.
- The ESP key to used for encryption of output datagrams.
- The authentication (AH) algorithm to be used.
- The AH key to be used for validation of input packets.
- The AH key to be used for generation of the authentication data for output datagrams.

The combination of a given Security Parameter Index and Destination IP address uniquely identifies a particular "Security Association." In one

embodiment, the sending firewall uses the sending userid and Destination Address to select an appropriate Security Association (and hence SPI value). The receiving firewall uses the combination of SPI value and Source address to obtain the appropriate Security Association.

5 A security association is normally one-way. An authenticated communications session between two firewalls will normally have two Security Parameter Indexes in use (one in each direction). The combination of a particular Security Parameter Index and a particular Destination Address uniquely identifies the Security Association.

10 More information on the specifics of an IPSEC FFE implementation can be obtained from the standards developed by the IPSEC work group and documented in *Security Architecture for IP* (RFC 1825) and in RFC's 1826-1829.

 When a datagram is received from unprotected network 16 or is to be
15 transmitted to a destination across unprotected network 16, the firewall must be able to determine the algorithms, keys, etc. that must be used to process the datagram correctly. In one embodiment, this information is obtained via a security association lookup. In one such embodiment, the lookup routine is passed several arguments: the source IP address if the datagram is being received
20 from network 16 or the destination IP address if the datagram is to be transmitted across network 16, the SPI, and a flag that is used to indicate whether the lookup is being done to receive or transmit a datagram.

 When an IPSEC datagram is received by firewall 18 from unprotected network 16, the SPI and source IP address are determined by looking in the
25 datagram. In one embodiment a Security Association Database (SADB) stored within firewall 18 is searched for the entry with a matching SPI. In one such embodiment, security associations can be set up based on network address as well as a more granular host address. This allows the network administrator to create a security association between two firewalls with only a couple of lines in
30 a configuration file on each machine. For such embodiments, the entry in the Security Association Database that has both the matching SPI and the longest

address match is selected as the SA entry. In another such embodiment, each SA has a prefix length value associated with the address. An address match on a SA entry means that the addresses match for the number of bits specified by the prefix length value.

5 There are two exceptions to this search process. First, when an SA entry is set marked as being dynamic it implies that the user of this SA may not have a fixed IP address. In this case the match is fully determined by the SPI value. Thus it is necessary that the SPI values for such SA entries be unique in the SADB. The second exception is for SA entries marked as tunnel mode entries.
10 In this case it is normally the case that the sending entity will hide its source address so that all that is visible on the public wire is the destination address. In this case, like in the case where the SA entries are for dynamic IP addresses, the search is done exclusively on the basis of the SPI.

 When transmitting a datagram across unprotected network 16 the SADB
15 is searched using only the destination address as an input. In this case the entry which has the longest address match is selected and returned to the calling routine.

 In one embodiment, if firewall 18 receives datagrams which are identified as either an IP_PROTO_IPSEC_ESP or IP_PROTO_IPSEC_AH
20 protocol datagram, there must be a corresponding SA in the SADB or else firewall 18 will drop the packet and an audit message will be generated. Such an occurrence might indicate a possible attack or it might simply be a symptom of an erroneous key entry in the Security Association Database.

 In a system such as system 10, application level gateway firewall 18 acts
25 as a buffer between unprotected network 16 and workstations such as workstation 20. Messages coming from unprotected network 16 are reviewed and a determination is made as to whether execution of an authentication and identification protocol is warranted. In contrast to previous systems, system 10
30 also performs this same determination on IPSEC-encrypted messages. If desired, the same authentication and identification can be made on messages to be transferred from workstation 20 to unprotected network 16. Figure 2

illustrates one way of authenticating both encrypted and unencrypted messages in a system such as system 10.

In the system of Figure 2 a network protocol stack 40 includes a physical layer 42, an Internet protocol (IP) layer 44, a Transport layer 46 and an application layer 48. Such a protocol stack exists, for instance on application level gateway firewall 18 of Figure 1. An application executing in application layer 48 can communicate to an application executing on another system by preparing a message and transmitting it through one of the existing transport services executing on transport layer 46. Transport layer 46 in turn uses a process executing in IP layer 44 to continue the transfer. Physical layer 42 provides the software needed to transfer data through the communication hardware (e.g., a network interface card or a modem). As noted above, IPSEC executes within IP layer 44. Encryption and authentication is transparent to the host as long as the network administrator has the Security Association Database correctly configured and a key management mechanism is in place on the firewall.

In application level gateway firewall 18, a proxy 50 operating within application layer 48 processes messages transferred between internal and external networks. All network-to-network traffic must pass through one of the proxies within application layer 48 before being the transfer across networks is allowed. A message arriving from external network 16 is examined at IP layer 44 and an SADB is queried to determine if the source address and SPI are associated with an SA. In the embodiment shown in Figure 2, an SADB Master copy 52 is maintained in persistent memory at application layer 48 while a copy 54 of SADB is maintained in volatile memory within the kernel. If the message is supposed to be encrypted, the message is decrypted based on the algorithm and key associated with the particular SA and the message is transferred up through transport layer 46 to proxy 50. Proxy 50 examines the source and destination addresses and the type of service desired and decides whether authentication of the sender is warranted. If so, proxy 50 initiates an authentication protocol. The protocol may be as simple as requesting a user

name and password or it may include a challenge/response authentication process. Proxy 50 also looks to see whether the message coming in was encrypted or not and may factor that into whether a particular type of authentication is needed. In Telnet, for instance, user name/password authentication may be sufficient for an FFE link while the security policy may dictate that a more stringent challenge/response protocol is needed for unencrypted links. In that case, proxy 50 will be a Telnet proxy and it will base its authentication protocol on whether the link was encrypted or not.

Since IPSEC executes within IP layer 44 there is no need for host firewalls to update their applications. Users that already have IPSEC available on their own host machine will, however, have to request that the firewall administrator set up SA's in the SADB for their traffic.

In the embodiment shown in Figure 2, a working copy 54 of the Security Association Database consisting of all currently active SA's is kept resident in memory for ready access by IP layer processing as datagrams are received and transmitted. In addition, a working master copy 52 of the SADB is maintained in a file in nonvolatile memory. During system startup and initialization processing the content of all of the required SA's in master SADB 52 is added to the working copy 54 stored in kernel memory.

In one embodiment, firewall 18 maintains different levels of security on internal and external network interfaces. It is desirable for a firewall to have different levels of security on both the internal and external interfaces. In one embodiment, firewall 18 supports three different levels, numbered 0 through 2. These levels provide a simple policy mechanism that controls permission for both in-bound and out-bound packets.

Level 0 - do not allow any in-bound or out-bound traffic unless there is a security association between the source and destination.

- Level 1 - Allow both in-bound and out-bound non-IPSEC traffic but force the use of IPSEC if a SA exists for the address. (To support this firewall 18 must look for a SA for each in-bound datagram.)

5 - Level 2 - allow NULL security associations to exist. NULL associations are just like normal security associations, except no encryption or authentication transform is performed on in-bound or out-bound packets that correspond to this NULL association. With Level 2 enabled, the machine will still receive unprotected traffic, but it will not transmit unless Level 1 is enabled.

The default protection level established when the Security Association Database (SADB) is initialized at boot time is 1 for in-bound traffic and 2 for out-bound traffic.

An Access Control List, or ACL, is a list of rules that regulate the flow of Internet connections through a firewall. These rules control how a firewall's servers and proxies will react to connection attempts. When a server or proxy 15 receives an incoming connection, it performs an ACL check on that connection.

An ACL check compares a set of parameters associated with the connection against a list of ACL rules. The rules determine whether the connection is allowed or denied. A rule can also have one or more side effects. A side effect causes the proxy to change its behavior in some fashion. For 20 example, a common side effect is to redirect the destination IP address to an alternate machine. In addition to IP connection attempts, ACL checks can also be made on the console logins and on logins made from serial ports. Finally, ACL checks can also be made on behalf of IP access devices, such as a Cisco box, through the use of the industry standard TACACS+ protocol.

25 In one embodiment, the ACL is managed by an acld daemon running in the kernel of firewalls 10 and 30. The acld daemon receives two types of requests, one to query the ACL and one to administer it. In one such embodiment, the ACL is stored in a relational database such as the Oracle database for fast access. By using such a database, query execution is 30 asynchronous and many queries can be executing concurrently. In addition, these types of databases are designed to manipulate long lists of rules quickly

and efficiently. These qualities ensure that a given query cannot hang up the process that issued the query for any appreciable time (> 1-2 seconds).

In one such embodiment, the database can hold up to 100,000 users and up to 10,000 hosts but can be scaled up to the capacity of the underlying
 5 database engine. The results of an ACL check is cached, allowing repeated checks to be turned around very quickly.

Applications on firewalls 10 and 30 can query `acld` to determine if a given connection attempt should be allowed to succeed. In one embodiment, the types of applications (i.e. "agents") that can make ACL queries can be divided
 10 into four classes:

- 1) Proxies. These allow connections to pass through firewall 10 or 30 in order to provide access to a remote service. They include `tnauthp` (authenticated telnet proxy), `pftp` (FTP proxy), `httpd` (HTTP proxy), and `tcpd` (TCP generic service proxy).
- 15 2) Servers. These provide a service on the firewall itself. They include `ftpd` and `httpd`.
- 3) Login agents. Login agent is a program on the firewall that can create a Unix shell. It is not considered a server because it cannot receive IP connections. One example is `/usr/bin/login` when used to create a dialup
 20 session or a console session on firewall 10 or 30. Another example is the command `role`.
- 4) Network Access Servers (NAS). NAS is a remote IP access device, typically a dialup box manufactured by such companies as Cisco or Bridge. The NAS usually provides dialup telnet service and may also
 25 provide SLIP or PPP service.

Proxies, servers, login agents, and NASes make queries to `acld` to determine if a given connection attempt should be allowed to succeed. All of the agents except NAS make their queries directly. NAS, because it is remote, must communicate via an auxiliary daemon that typically uses an industry standard
 30 protocol such as RADIUS or TACACS+. The auxiliary daemon (e.g., `tacadd`) in turn forwards the query to local `acld`.

As a side effect of the query, `acld` tells the agent if authentication is needed. If no authentication is needed, the connection proceeds immediately. Otherwise `acld` provides (as another side effect) a list of allowed authentication methods that the user can choose from. The agent can present a menu of choices
5 or simply pick the first authentication method by default. Typical authentication methods include plain password, SNK DSS, SDI SecurID, LOCKout DES, and LOCKout FORTEZZA. In one embodiment, the list of allowed authentication methods varies depending on the host name, user name, time of day, or any combination thereof.

10 In the case of a Level 0 policy, it would be safe to assume that all incoming traffic is encrypted or authenticated. In the case of Levels 1 through 2, a determination must be made whether or not a security association exists for a given peer. Otherwise an application may believe that in-bound traffic has been authenticated when it really has not. (That is why it is necessary to look for an
15 SA on input of each non-IPSEC datagram.)

In one embodiment, a flag which accompanies the message as it is sent from IP layer 44 to proxy 50 indicates whether the incoming message was or was not encrypted. In another embodiment, proxy 50 accesses Security Association Database 54 (the table in the kernel can be queried via an SADB routing socket
20 (PF-SADB)) to determine whether or not a security association exists for a given peer.. The SADB socket is much like a routing socket found in the stock BSD 4.4 kernel (protocol family PF-ROUTE) except that PF-SADB sockets are used to maintain the Security Association Database (SADB) instead of the routing table. Because the private keys used for encryption, decryption, and keyed
25 authentication are stored in this table, access must be strictly prohibited and allowed to only administrators and key management daemons. Care must be taken when allowing user-level daemons access to `/dev/mem` or `/dev/kmem` as well, since the keys are stored in kernel memory and could be exposed with some creative hacking.

30 In one embodiment, a command-line tool called `sadb` is used to support the generation and maintenance of in-kernel version 54 of SADB. The primary

interface between this tool and the SADB is the PF-SADB socket. The kernel provides socket processing to receive client requests to add, update, or change entries in in-kernel SADB 54. As noted above, the default protection level established when the Security Association Database (SADB) is initialized at boot
 5 time is 1 for in-bound traffic and 2 for out-bound traffic. This may be changed by the use of the `sadb` command.

The existing `sadb` command was derived from the NIST implementation of IPSEC. As noted above, this tool is much like `route` in that it uses a special socket to pass data structures in and out of the kernel. There are three commands
 10 recognized by the `sadb` command: *get*, *set*, *delete*. The following simple shell script supports adding and removing a single SA entry to SADB 54. It shows one embodiment of a parameter order for adding a SA to the SADB.

```

# ! /bin/sh
15 if [ $# -ne 1 ]
    then
        echo "usage: $0 <on>|<off>" >&2
        exit 1
    fi
20 ONOFF=$1

addsa ()
{
    IPADDRESS=$2
25 PEERADDRESS=0.0.0.0
    PREFIXLEN=0           # Num of bits, 0 => full 32
    bit match
    LOCALADDRESS=0.0.0.0
    REALADDRESS=0.0.0.0
30 PORT=0
    PROTOCOL=0
    UID=0
    DESALG=1             # I = DES-CBC
    IVLEN=4              # bytes
35 DESKEY=0b0b0b0b0b0b0b0b
    DESKEYLEN=8          # bytes
    AHALG=1              # 1 = MD5
    AHKEY=30313233343536373031323334353637
    AHKEYLEN=16         # bytes
40 LOCAL_SPI=$1
  
```

```

PEER_SPI=$1
TUNNEL_MODE=0
AHRESULTLEN=4
COMBINED_MODE=1          # On output, 1 = ESP, then
5 AH; 0 = AH, then ESP
DYNAMIC_FLAG=0

if [ "$SONOFF" = "on"
then
10     ./sadb add dst $IPADDRESS $PREFIXLEN $LOCAL_SPI
      $UID $PEERADDRESS $PEER_SPI $TUNNEL_MODE $LOCALADDRESS
      $REALADDRESS $PROTOCOL $PORT $DESALG $IVLEN $DESKEYLEN
      $DESKEY $DESKEYLEN $DESKEY $AHALG $AHKEYLEN $AHKEY
15 $AHKEYLEN $AHKEY $AHRESULTLEN $COMBINED_MODE
      $DYNAMIC_FLAG
    else
      ./sadb delete dst $IPADDRESS $LOCAL-SPI
    fi
  }
20
#   Get down to work:
addsa 500 172.17.128.115          # number6.sctc.com

```

The current status of in-kernel SADB 54 can be obtained with the `sadb` command. The `get` option allows dumping the entire SADB or a single entry. In one embodiment, the complete dump approach uses `/dev/kmem` to find the information. The information may be presented as follows:

```

30 # sadb get dst
Local-SPI Address-Family Destination-Addr
Preflx_length UID
Peer-Address Peer-SPI Transport-Type
Local-Address Real-Address
35 Protocol Port
ESP_Alg_ID ESP_IVEC_Length
ESP_Enc_Key_length ESP_Enc_ESP_Key
ESP_Dec_Key_length ESP_Dec_ESP_Key
AH_Alg_ID AH_Data_Length
40 AH_Gen_Key_Length AH_Gen_Key
AH_Check_Key_Length AH_Check_Key
Combined_Mode Dynamic_Flag

```

```

-----
-
500 INET: number6.sctc.com 0 0
      0.0.0.0 500 Transport(0) 0
5    0.0.0.0 0.0.0.0
      None None
      DES/CBC-RFC1829(1) 4
          8 0b0b0b0b0b0b0b0b
          8 0b0b0b0b0b0b0b0b
10   MDS-RFC1828(1) 4
          16 30313233343536373031323334353637
          16 30313233343536373031323334353637
      ESP+AH(1) 0
501 INET: spokes.sctc.com 0 0
15   0.0.0.0 501 Transport(0) 0
      0.0.0.0.0.0.0.0.0
      None None
      DES/CBC-RFC1829(1) 4
          8 0b0b0b0b0b0b0b0b
20   8 0b0b0b0b0b0b0b0b
      MDS-RFC1828(1) 4
          16 30313233343536373031323334353637
          16 30313233343536373031323334353637
25   ESP+AH(1) 0
End of list.

```

When a new entry is added to in-kernel SADB 54, the add process first checks to see that no existing entry will match the values provided in the new entry. If no match is found then the entry is added to the end of the existing SADB list.

To illustrate the use and administration of an FFE, we'll go through an example using FFE 70 in Figure 3. Firewalls 14 and 18 are both application level gateway firewalls implemented according to the present invention. Workstations H2 and H3 both want to communicate with H1. For the administrator of firewalls 14 and 18, this is easy to accomplish. The administrator sets up a line something like this (we'll only show the IP address part and SPI parts of the SA, since they're the trickiest values to configure. Also, assume that we are using tunnel mode):

```

40 # Hypothetical SW1 Config File

```

```

#
# Fields are laid out in the following manner:
# srcaddrornet= localSPI= peeraddr= peerSPI=
# realsrcaddr= localaddr= key=
5
# The following entry sets up a tunnel between hosts
# behind SW1
# and hosts behind SW2.
src=172.16.0.0 localSPI=666 peer=192.168.100.5
10 peerSPI=777 \
    realsrcaddr=192.168.100.5 localaddrs=0.0.0.0
    key=0xdeadbeeffadebabe

# Hypothetical SW2 Config File
15 #
# Fields are laid out in the following manner:
# srcaddrornet= localSPI= peeraddr= peerSPI=
# realsrcaddr= localaddr= key=

20 # The following entry sets up a tunnel between hosts
# behind SW1 and
# hosts behind SW2.
src=172.17.0.0 localSPI=777 peer=192.168.20.1
peerSPI=666 \
25 realsrcaddr=192.168.20.1 localaddr=0.0.0.0 \
    key=0xdeadbeeffadebabe

```

With this setup, all traffic is encrypted using one key, no matter who is talking to whom. For example, traffic from H2 to H1 as well as traffic from H3 to H1 will be encrypted with one key. Although this setup is small and simple, it may not be enough.

What happens if H2 cannot trust H3? In this case, the administrator can set up security associations at the host level. In this case, we have to rely on the SPI field of the SA, since the receiving firewall cannot tell from the datagram header which host behind the sending firewall sent the packet. Since the SPI is stored in IPSEC datagrams, we can do a lookup to obtain its value. Below are the sample configuration files for both firewalls again, but this time, each host combination communicates with a different key. Moreover, H2 excludes H3 from communications with H1, and H3 excludes H2 in the same way.

40

```

# Hypothetical SW1 Config File
#
# Fields are laid out in the following manner:
# srcaddrornet= localSPI= peeraddr= peerSPI=
5 realsrcaddr= localaddr= key=

# The following entry sets up a secure link between H2
and H1
src=172.16.0.2 localSPI=666 peer=192.168.100.5
10 peerSPI=777 \
    realsrcaddr=192.168.100.5
localaddrs=178.17.128.71 \
    key=0x0a0a0a0a0a0a0a0a

15 # The following entry sets up a secure link between H3
and H1
src=172.16.0.1 localSPI=555 peer=192.168.100.5
peerSPI=888 \
    realsrcaddr=192.168.100.5
20 localaddrs=178.17.128.71 \
    key=0x0b0b0b0b0b0b0b0b

# Hypothetical SW2 Config File
#
# Fields are laid out in the following manner:
# srcaddrornet= localSPI= peeraddr= peerSPI=
# realsrcaddr= localaddr= key=

# The following entry sets up a secure link between H2
30 and H1
src=172.17.128.71 localSPI=777 peer=192.168.20.1
peerSPI=666 \
    realsrcaddr=192.168.20.1 localaddrs=172.16.0.2 \
    key=0x0a0a0a0a0a0a0a0a
35

# The following entry sets up a secure link between H3
and H1
src=172.17.128.71 localSPI=888 peer=192.168.20.1
peerSPI=555 \
40 realsrcaddr=192.168.20.1 localaddrs=172.16.0.1 \
    key=0x0b0b0b0b0b0b0b0b

```

Figure 4 is a block diagram showing in more detail one embodiment of an IPSEC-enabled application level gateway firewall 18. Application level gateway firewall 18 provides access control checking of both encrypted and

unencrypted messages in a more secure environment due to its network-separated architecture. Network separation divides a system into a set of independent regions or burbs, with a domain and a protocol stack assigned to each burb. Each protocol stack 40x has its own independent set of data structures, including routing information and protocol information. A given socket will be bound to a single protocol stack at creation time and no data can pass between protocol stacks 40 without going through proxy space. A proxy 50 therefore acts as the go-between for transfers between domains. Because of this, a malicious attacker who gains control of one of the regions is prevented from being able to compromise processes executing in other regions. Network separation and its application to an application level gateway is described in "SYSTEM AND METHOD FOR ACHIEVING NETWORK SEPARATION", U.S. Application No. 08/599,232, filed February 9, 1996 by Gooderum et al.

In the system shown in Figure 4, the in-bound and out-bound datagram processing of a security association continues to follow the conventions defined by the network separation model. Thus all datagrams received on or sent to a given burb remain in that burb once decrypted. In one such embodiment SADB socket 78 has been defined to have the type 'sadb'. Each proxy 50 that requires access to SADB socket 78 to execute its query as to whether the received message was encrypted must have create permission to the sadb type.

The following is list of specific requirements that a system such as is shown in Figure 4 must provide. Many of the requirements were discussed in the information provided earlier in this document.

1. Firewall applications may query the IPSEC subsystem to determine if traffic with a given address is guaranteed to be encrypted.
2. Receipt of an unencrypted datagram from an address that has a SA results in the datagram being dropped and an audit message being generated.
3. On receipt of encrypted protocol datagrams the SADB searches will be done using the SPI as the primary key. The source address will a secondary key. The SA returned by the search will be the SA which matches the SPI exactly and has the longest match with the address.

4. A search of the SADB for a SPI that finds an entry that is marked as SA for a dynamic IP will not consider the address in the search process.
5. A search of the SADB for a SPI that finds an entry that is marked as a SA for a tunnel mode connection will to consider the address if it is (0.0.0.0) i.e INADDR.
6. On receipt of a non-IPSEC datagram the SADB will be searched for an entry that matches the src address. If a SA is found the datagram will be dropped and an audit message sent.
7. SADB searches on output will be done using the DST address as key. If more than one SA entry in the SADB has that address the first one with the maximum address match will be returned.
8. The SADB must be structured so that searches are fast regardless if the search is done by SPI or by address.
9. The SADB must provide support for connections to a site with a fixed SPI but changing IP address. SA entries for such connections will be referred to as Dynamic Address Sites, or just Dynamic entries.
10. When a dynamic entry is found by a SPI search, the current datagram's SRC address, which is required to ensure that the return datagrams are properly encrypted, will be recorded in the SA only after the AH checking has passed successfully. (This is because if the address is recorded before AH passes then an attacker can cause return packets of an outgoing connection to be transmitted in the clear.)
11. A failure of an AH check on a dynamic entry results in an audit message.
12. In an embodiment where the firewall requires that all connections use both AH and ESP, on receipt the order should be AH first ESP second.
13. The processing structure on both input and output should try to minimize the number of SADB required lookups.

Returning to Figure 4, in one embodiment firewall 18 includes a crypto engine interface 80 used to encrypt an IPSEC payload. Crypto engine interface 80 may be connected to a software encryption engine 82 or to a hardware

encryption engine 84. Engines 82 and 84 perform the actual encryption function using, for example, DES-CBC. In addition, software encryption engine 82 may include the keyed MD5 algorithm used for AH.

In one embodiment, crypto engine interface 80 is a utility which provides a consistent interface between the software and hardware encryption engines. As shown in Figure 4, in one such embodiment interface 80 only supports the use of the use of hardware cryptographic engine 84 for IPSEC ESP processing. The significant design issue that interface 80 must deal with is that use of a hardware encryption engine requires that the processing be down in disjoint steps operating in different interrupt contexts as engine 84 completes the various processing steps.

The required information is stored in a request structure that is bound to the IP datagram being processed. The request is of type `crypto_request_t`. This structure is quite large and definitely does not contain a minimum state set.

In addition to the definition of the request data structure, this software implementing interface 80 provides two functions which isolate the decision of which cryptographic engine to use. The `crypt_des_encrypt` function is for use by the IP output processing to encrypt a datagram. The `crypt_des_decrypt` function is for use by the IP input processing to decrypt a datagram. If hardware encryption engine 84 is present and other hardware usage criteria are met the request is enqueued on a hardware processing queue and a return code indicating that the cryptographic processing is in progress is returned. If software engine 82 is used, the return code indicates that the cryptographic processing is complete. In the former case, the continuation of the IP processing is delayed until after hardware encryption is done. Otherwise it is completed as immediately in the same processing stream.

There are two software cryptographic engines 82 provided in the IPSEC software. One provides the MD5 algorithm used by the IPSEC AH processing, and the other provides the DES algorithm used by the IPSEC ESP processing. This software can be obtained from the US Government IPSEC implementation.

In one embodiment hardware cryptographic engine 84 is provided by a Cylink SafeNode processing board. The interface to this hardware card is provided by the Cylink device driver. A significant aspect of the Cylink card that plays a major part in the design of the IPSEC Cylink driver is that the card
5 functions much like a low level subroutine interface and requires software support to initiate each processing step. Thus to encrypt or decrypt an individual datagram there are a minimum of two steps, one to set the DES initialization vector and one to do the encryption. Since the IP processing can not suspend
10 itself and wait while the hardware completes and then be rescheduled by the hardware interrupt handler, in one embodiment a finite state machine is used to tie sequences of hardware processing elements together. In one such embodiment the interrupt handler looks at the current state, executes a defined after state function, transitions to the state and then executes that state's start function.

15 One function, `cyl_enqueue_request`, is used to initiate either an encrypt or a decrypt action. This function is designed to be called by cryptographic engine interface 80. All of the information required to initiate the processing as well as the function to be performed after the encryption operation is completed is provided in the request structure. This function will enqueue the
20 request on the hardware request queue and start the hardware processing if necessary.

A system 30 which can be used for firewall-to-workstation encryption is shown in Figure 5. In Figure 5, system 30 includes a workstation 12 communicating through a firewall 14 to an unprotected network 16 such as the
25 Internet. System 30 also includes a workstation 32 communicating directly with firewall 14 through unprotected network 16. Firewall 14 is an application level gateway incorporating IPSEC handling as described above. (It should be noted that IPSEC security cannot be used to authenticate the personal identity of the sender for a firewall to firewall transfer. When IPSEC is used, however, on a
30 single user machine such as a portable personal computer, IPSEC usage should

be protected with a personal identification number (PIN). In these cases IPSEC can be used to help with user identification to the firewall.)

According to the IPSEC RFC's, you can use either tunnel or transport mode with this embodiment based on your security needs. In certain situations,
5 the communications must be sent in tunnel mode to hide unregistered addresses.

Although specific embodiments have been illustrated and described herein, it will be appreciated by those of ordinary skill in the art that any arrangement which is calculated to achieve the same purpose may be substituted for the specific embodiment shown. This application is intended to cover any
10 adaptations or variations of the present invention. Therefore, it is intended that this invention be limited only by the claims and the equivalents thereof.

What is claimed is:

1. A method of regulating the flow of messages through a firewall having a network protocol stack, wherein the network protocol stack includes an Internet Protocol (IP) layer, the method comprising the steps of:
 - 5 determining, at the IP layer, if a message is encrypted;
 - if the message is not encrypted, passing the unencrypted message up the network protocol stack to an application level proxy; and
 - 10 if the message is encrypted, decrypting the message and passing the decrypted message up the network protocol stack to the application level proxy, wherein the step of decrypting the message includes the step of executing a procedure at the IP layer to decrypt the message.

2. A method of authenticating the sender of a message within a computer system having a network protocol stack, wherein the network protocol stack includes an Internet Protocol (IP) layer, the method comprising the steps of:
 - 15 determining, at the IP layer, if the message is encrypted;
 - if the message is encrypted, decrypting the message, wherein the step of decrypting the message includes the step of executing a process at the IP layer to
 - 20 decrypt the message;
 - passing the decrypted message up the network protocol stack to an application level proxy;
 - determining an authentication protocol appropriate for the message; and
 - 25 executing the authentication protocol to authenticate the sender of the message.

3. The method according to claim 2 wherein the step of determining an authentication protocol appropriate for the message includes the steps of:
 - 30 determining a source IP address associated with the message; and
 - determining the authentication protocol associated with the source IP address.

4. The method according to claim 2 wherein the message includes security parameters index and wherein the step of determining an authentication protocol appropriate for the message includes the steps of:

5 determining the authentication protocol associated with a dynamic IP address, wherein the step of determining the authentication protocol includes the step of looking up a security association based on the security parameters index; determining a current address associated with the dynamic source IP address; and binding the current address to the security parameters index.

10

5. A firewall, comprising:

a first communications interface;

a second communications interface;

a network protocol stack connected to the first and the second

15 communications interfaces, wherein the network protocol stack includes an Internet Protocol (IP) layer and a transport layer;

a decryption procedure, operating at the IP layer, wherein the decryption procedure decrypts encrypted messages received at one of said first and second communications interfaces and outputs decrypted messages; and

20 a proxy, connected to the transport layer of said network protocol stack, wherein the proxy receives decrypted messages from the decryption procedure and executes an authentication protocol based on the content of the decrypted message.

25 6. A firewall, comprising:

a first communications interface;

a second communications interface;

a first network protocol stack connected to the first communications interface, wherein the first network protocol stack includes an Internet Protocol

30 (IP) layer and a transport layer;

a second network protocol stack connected to the second communications interface, wherein the second network protocol stack includes an Internet Protocol (IP) layer and a transport layer;

5 a decryption procedure, operating at the IP layer of the first network protocol stack, the decryption procedure receiving encrypted messages received by said first communications interface and outputting decrypted messages; and

a proxy, connected to the transport layers of said first and second network protocol stacks, the proxy receiving decrypted messages from the decryption procedure and executing an authentication protocol based on the content of the
10 decrypted message.

7. The firewall according to claim 6 wherein the firewall further includes:
a third communications interface; and

a third network protocol stack connected to the third communications
15 interface and to the proxy, wherein the third network protocol stack includes an Internet Protocol (IP) layer and a transport layer and wherein the second and third network protocol stacks are restricted to first and second burbs, respectively.

20 8. A method of establishing a virtual private network between a first and a second network, wherein each network includes an application level gateway firewall which uses a proxy operating at the application layer to process traffic through the firewall, wherein each firewall includes a network protocol stack and wherein each network protocol stack includes an Internet Protocol (IP) layer, the
25 method comprising the steps of:

transferring a connection request from the first network to the second network;

determining, at the IP layer of the network protocol stack of the second network's firewall, if the connection request is encrypted;

if the connection request is encrypted, decrypting the request, wherein the step of decrypting the request includes the step of executing a procedure at the IP layer of the second network's firewall to decrypt the message;

- 5 passing the connection request up the network protocol stack to an application level proxy;
- determining an authentication protocol appropriate for the connection request;
- executing the authentication protocol to authenticate the connection request; and
- 10 if the connection request is authentic, establishing an active connection between the first and second networks.

9. The method according to claim 8 wherein the step of executing the authentication protocol includes the step of executing program code within the firewall of the second network to mimic a challenge/response protocol executing on a server internal to the second network.

15

10. The method according to claim 8 wherein the step of executing the authentication protocol includes the step of executing program code to execute the authentication protocol in line to the session.

20

11. The method according to claim 8 wherein the step of determining an authentication protocol includes the step of determining if the connection request arrived encrypted and selecting the authentication protocol based on whether the connection request was encrypted or not encrypted.

25



Application No: GB 9719816.2
Claims searched: 1-11

Examiner: B.J.SPEAR
Date of search: 21 January 1998

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.P): H4P (PPEB,PDCSA,PDCSC)

Int Cl (Ed.6): H04L 9/00, 9/32, 29/06, 29/08

Other: Online:WPI, INSPEC

Documents considered to be relevant:

Table with 3 columns: Category, Identity of document and relevant passage, Relevant to claims. Rows include XP WO97/26734A1, XP WO97/26731A1, XP WO97/26735A1, XP WO97/23972A1, and XP WO97/13340A1.

Legend table with 2 columns: Symbol and Description. Symbols include X, Y, &, A, P, E.



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification ⁶ : H04Q 11/04, H04L 12/22</p>	<p>A1</p>	<p>(11) International Publication Number: WO 98/27783 (43) International Publication Date: 25 June 1998 (25.06.98)</p>
<p>(21) International Application Number: PCT/IB97/01563 (22) International Filing Date: 12 December 1997 (12.12.97) (30) Priority Data: 08/769,649 19 December 1996 (19.12.96) US (71) Applicant (for all designated States except US): NORTHERN TELECOM LIMITED [CA/CA]; World Trade Center of Montreal, 8th floor, 380 St. Antoine Street West, Montreal, Quebec H2Y 3Y4 (CA). (72) Inventors; and (75) Inventors/Applicants (for US only): TELLO, Antonio, G. [US/US]; 114 Fountain Hills Drive, Garland, TX 75044 (US). HUI, Margaret [US/US]; 9920 Forest Lane #208, Dallas, TX 75243 (US). HOLMES, Kim [US/US]; 5409 Scenic Drive, Rowlett, TX 75088 (US). (74) Agents: MCCOMBS, David et al.; Haynes and Boone, L.L.P., Suite 3100, 901 Main Street, Dallas, TX 75202-3789 (US).</p>	<p>(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG). Published <i>With international search report.</i></p>	

(54) Title: VIRTUAL PRIVATE NETWORK SERVICE PROVIDER FOR ASYNCHRONOUS TRANSFER MODE NETWORK

(57) Abstract

A virtual private network service provider is used to transfer data over a data network to a final destination, with third-party billing. The method comprises the steps of: prompting the user at a data terminal to select a destination, password, and call type; sending a set-up message to the data network; selecting a virtual private network provider through the data network; the virtual private network provider giving an encryption key to the user, and then prompting the user for a password and a user identification; encrypting the password, and sending the user identification and the encrypted password to the virtual private network provider; the virtual private network provider decrypting the encrypted password, and verifying the password; the virtual private network provider providing an authorization code; and the data terminal transferring the data through the data network to the final destination, using the authorization code.

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	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

VIRTUAL PRIVATE NETWORK SERVICE PROVIDER FOR ASYNCHRONOUS TRANSFER MODE NETWORK

Technical Field

The invention relates generally to asynchronous transfer mode ("ATM") networks and virtual private networks ("VPN"), such as those offered by MCI and Sprint, and, more particularly, to a method of using a VPN to transfer data over a data network, with third-party billing.

Background of the Invention

Telephone service providers offer third-party billing. For example, local and long distance telephone companies offer calling cards for third party billing.

VPNs exist to provide the sense of a private network among a company's locations. The lines/trunks of a VPN are actually shared among several companies, to reduce costs, yet to each company the VPN appears to be that company's own private network. However, a user at a remote data terminal, such as a portable computer in a hotel room, can not immediately charge his company for the access time to a data net, such as the Internet. Instead, his access time is charged to his hotel room, and so he must pay the inflated rates that hotels charge for phone service.

What is needed is a VPN service provider that offers remote access for users belonging to a VPN, user authorizations to prevent delinquent access into the VPN, and convenient third-party billing.

Summary of the Invention

The present invention, accordingly, provides a system and method for using a VPN service provider to transfer data over a data network to a final destination, with third-party billing. The method comprises the steps of: prompting the user at a data terminal to select a destination, password, and call type; selecting a VPN through the data network; giving an encryption key to the user, and then prompting the user for a password and a user identification; verifying the password, and providing an authorization code to

the user; and allowing the user to transfer the data through the data network to the final destination, using the authorization code.

In another feature of the invention, the method further comprises negotiating for more bandwidth for the user, and including within the authorization code a grant of additional bandwidth.

In another feature of the invention, the method further comprises encrypting the user's password, and sending the user identification and the encrypted password to the VPN service provider.

In another feature of the invention, the method further comprises a step of sending a set-up message to the data network.

In another feature of the invention, the method further comprises a step of the VPN service provider decrypting the encrypted password.

A technical advantage achieved with the invention is that it shifts or defers costs from an end user to a bulk purchaser of data network services. Another technical advantage achieved with the invention is that it permits end users mobility while attaining a virtual appearance on a corporate intranet.

Brief Description of the Drawings

Fig. 1 is a system block diagram of a VPN service provider of the present invention.

Fig. 2 is a flow chart depicting the method of the present invention, as implemented by application software on a user terminal.

Fig. 3 is the initial screen display of the user interface of the application software.

Figs. 4A and 4B are call flow diagrams, illustrating the preferred sequence of steps of the method of the present invention.

Figs. 5A, 5B, 5C, 5D, 5E, and 5F comprise a flow chart depicting the method of the present invention, as implemented by switching control point software.

Description of the Preferred Embodiment

In Fig. 1, the VPN service provider system of the present invention is designated generally by a reference numeral 10. The VPN service provider system 10 includes a VPN 12. The VPN 12 may be a corporate, government, association, or other organization's telephone/data line network. The VPN service provider system 10 also includes access lines 13 from the VPN 12 to a data network 14, such as the Internet, or an ATM network. The VPN service provider system 10 also includes access lines 16 from the data network 14 to a long distance phone company 18, such as AT&T, MCI, or Sprint. The VPN service provider system 10 also includes access lines 20 from the data network 14 to a called party 22, such as, for example, American Express reservations service. The VPN service provider system 10 also includes access lines 24 from the data network 14 to a remote user terminal 26, such as a portable computer in a hotel room. The user terminal 26 includes user application software 28, which provides the interface for the user to enter the number to be called, the user identification number, and the user's authorization code. The VPN service provider system 10 also includes VPN service provider software 30, located in a switching control point (SCP) device 32, which, in the preferred embodiment may be physically located anywhere. The SCP 32 connects to the data network 14 via access lines 36. One possible physical location for the SCP 32 is on the premises of a local phone company central switch building 34. However, even when located within the building 34, the SCP 32 connects to the local phone company switches via the data network 14. The local phone company switches connect to the data network 14 via access lines 38.

In an alternate embodiment, the VPN service provider software 30 and the SCP device 32 may be located on the premises of an independent provider of local phone service, or on the premises of an independent VPN service provider.

Referring now to Fig. 2, the application software 28 begins the data transfer process in step 50. In step 52, the user is presented with a screen display.

Referring now to Fig. 3, a screen display 100 displays the following information requests: whether the call is a direct call 102 or a VPN call 104, the number the user desires to call 106, the VPN user ID 108, and the user password 110. The user is also presented with the option to make the call 112, or to quit 114.

Referring back to Fig. 2, in step 54 the user terminal sends to the SCP 32 the information captured through the graphical user interface ("GUI") in step 52 within a user network interface ("UNI") setup message. In step 56 the user terminal 26 waits for a connect message from the SCP 32. In step 58 the user terminal 26 determines if a connection was made. If no connection was made, then in step 60 the user application software 28 displays an error message to the user, and returns to step 50 to begin again the data transfer process.

If a connection was made, then in step 62 the user terminal 26 sends the VPN user ID to the SCP 32. In step 64 the user terminal 26 waits for an encryption key from the SCP 32. In step 66, having received the encryption key from the SCP 32, the user application software 28 encrypts the user's password, and sends it to the SCP 32. In step 68 the user terminal 26 waits for authentication of the user. In step 70 the user application software 28 determines if the SCP 32 authorizes the user to make the call.

If the user is not authorized, then in step 72 the user terminal 26 displays an error message, terminates the connection, blanks the screen display 100, and returns to step 50 to begin again the data transfer process. If the user is authorized, then in step 74 the VPN service provider software 30 sets up the billing, and authorizes it. In step 76 the user terminal 26 sends a "release", meaning to terminate or disconnect the connection, to the SCP 32. In step 78 the user terminal 26 sends a setup message to the number listed by

the user as the "number to call", that is, to the final destination. In step 80 the user terminal 26 waits for a connection. In step 82 the user terminal 26 determines if a connection was made.

If a connection to the final destination was not made, then the user application software 28 returns to step 72, in which step the user terminal 26 displays an error message, terminates the connection, blanks the screen display 100, and returns to step 50 to begin again the data transfer process. If a connection to the final destination was made, then in step 84 the user terminal 26 exchanges user data, services, and/or value added or user specific applications with the computer at the address, that is, the telephone number, of the final destination. In step 86 the user selects the option presented to him to release, or terminate, the call. In step 88 the user terminal 26 sends a release message to the final destination. In step 90 the data network 14 sends billing information to the SCP 32. In step 92 the application software 28 ends the data transfer process.

Fig. 4A and Fig. 4B are call flow diagrams, showing the sequence of messages in the method of the preferred embodiment. These diagrams present the same method as the flow chart of Fig. 2. The horizontal arrows represent the messages sent and received. The vertical lines represent the various devices involved in sending and receiving the messages. For example, the top left arrow in Fig. 4A represents a message sent from the user terminal 26, labeled "Macintosh" in Fig. 4A, to an interface with a public network. The user terminal 26 can be any brand of a work station computer, a desktop computer, a laptop computer, or even a notebook computer. The interface could be any interface, but in the example of Fig. 4A and Fig. 4B, the interface is imagined to be at a hotel, where a business traveler is using the method of the present invention. Thus, the interface is labeled "Hotel ATM Interface", which is not shown in Fig. 1. The vertical line labeled "Public ATM Network" is the same as the data network 14 in Fig. 1. The vertical line labeled "Moe's VPN Service" represents the VPN service provider software 30

within the SCP 32. The vertical line labeled "Travel ATM Interface" is not shown in Fig. 1, but is located between the called party 22 and the data network 14. The vertical line labeled "Travel Service" is one example of the called party 22 shown in Fig. 1. In the example of Fig. 4A and Fig. 4B, the business traveler is imagined to be using the method of the present invention to contact a travel service to make reservations for his next airline flight. In Figs. 4A and 4B the designation "Ack" represents "acknowledge", and the designation "Cmp" represents "complete".

Referring now to Fig. 5, the VPN service provider software 30 begins the data transfer process in step 300 by waiting for an event. The event it waits for is a setup message on a signaling port of the SCP 32, to be received from the user terminal 26. In step 302, having monitored the signaling ports, and the SCP 32 having received a setup message, the VPN service provider software 30 assigns a call condense block ("CCB") to the setup message, based on a call reference number. The CCB is a software data structure for tracking resources associated with the call. The call reference number is a number, internal to the SCP, for tracking calls. In step 304 the VPN service provider software 30 compiles the connect message. In step 306 the VPN service provider software 30 sends a connect message to the calling address, that is, the hotel room from which the user is calling. In step 308 the VPN service provider software 30 condenses, that is, it remains in a wait state for that call.

Referring now to Fig. 5B, in step 310 the VPN service provider software 30 waits for an event by monitoring the signaling ports of the SCP 32. After the SCP 32 receives a connect acknowledge message from the user terminal 26, then in step 312 the VPN service provider software 30 accesses the CCB, based on the call reference number. In step 314 the VPN service provider software 30 condenses.

Referring now to Fig. 5C, in step 316 the VPN service provider software 30 waits for dialog on a data port of the SCP 32. After the SCP 32 receives a

VPN ID on a data port, the VPN service provider software 30 verifies the VPN ID in step 318. In step 320 the VPN service provider software 30 determines if the VPN ID is valid. If the VPN ID is not valid, then in step 322 the SCP 32 sends a reject message over an assigned switch virtual circuit ("SVC"). The SVC is a channel over the data network 14. In step 324 the VPN service provider software 30 waits for dialog. In step 326, because the VPN ID is valid, the VPN service provider software 30 assigns an encryption key to the user terminal 26, in step 328 sends the encryption key over the assigned SVC to the user terminal 26, and in step 330 waits for dialog.

Referring now to Fig. 5D, in step 332 the VPN service provider software 30 waits for dialog. When the SCP 32 receives the encrypted password from the user terminal 26 at a data port, then in step 334 the VPN service provider software 30 verifies the password, and determines in step 336 if the password is valid. If the password is not valid, then in step 338 the SCP 32 sends a reject message over the assigned SVC to the user terminal, and in step 340 waits for dialog. If the password is valid, then in step 342 the VPN service provider software 30 assigns an authorization token to the user terminal 26, in step 344 sends the token over an assigned SVC to the user terminal 26, and in step 346 waits for dialog.

Referring now to Fig. 5E, in step 348 the VPN service provider software 30 waits for an event. When the VPN service provider software 30 senses that the SCP 32 has received on a signaling port a release message from the user terminal 26, then in step 350 the VPN service provider software 30 accesses the CCB, based on the call reference number of the user terminal 26, in step 352 compiles a release complete message, in step 354 sends a release complete message to the user terminal 26, and in step 356 condenses.

Referring now to Fig. 5F, in step 358 the VPN service provider software 30 waits for an event. When the VPN service provider software 30 senses that the SCP 32 has received on a signaling port a third-party billing setup message from the user terminal 26, then in step 360 the VPN service provider

software 30 verifies the token just received from the user terminal 26, to determine, in step 362, if it is the same token that the VPN service provider software 30 sent to the user terminal 26 in step 344. If the token is not valid, then in step 364 the SCP 32 sends a release message to the terminal 26, and in step 366 condenses. If the token is valid, then in step 368 the SCP 32 sends a modified third-party billing setup message to the data network 14, and in step 370 condenses.

Although an illustrative embodiment of the invention has been shown and described, other modifications, changes, and substitutions are intended in the foregoing disclosure. Accordingly, it is appropriate that the appended claims be construed broadly and in a manner consistent with the scope of the invention.

WHAT IS CLAIMED IS:

1. A computerized method of a virtual private network service provider with third party billing, using a virtual private network to transfer data over a data network to a final destination, the method comprising the steps of:

- a. prompting the user at a data terminal to select a destination, password, and call type;
- b. selecting a virtual private network through the data network;
- c. giving an encryption key to the user, and then prompting the user for a password and a user identification;
- d. verifying the password, and providing an authorization code to the user; and
- e. allowing the user to transfer the data through the data network to the final destination, using the authorization code.

2. The method of claim 1, wherein step (d) further comprises negotiating for more bandwidth for the user, and including within the authorization code a grant of additional bandwidth.

3. The method of claim 2, wherein step (c) further comprises encrypting the user's password, and sending the user identification and the encrypted password to the virtual private network service provider.

4. The method of claim 3, further comprising, after step (a), the step of sending a set-up message to the data network.

5. The method of claim 4, further comprising, after step (c), the step of the virtual private network service provider decrypting the encrypted password.

6. An apparatus for providing a datalink connection from a user terminal to a data network and to a virtual private network, with third party billing, comprising:

- a. an interface between the user terminal and the data network;

- b. a switching control point device connected to the data network, the switching control point device connected to a computer; and
 - c. a computer-readable medium encoded with a method of using the virtual private network and the data network, with third party billing, the computer-readable medium accessible by the computer.
7. The apparatus of claim 6, wherein the method comprises negotiating for more bandwidth for the user, and including within an authorization code a grant of additional bandwidth.
8. The apparatus of claim 7, wherein the method further comprises encrypting a user's password, and temporarily storing the user identification and the encrypted password.
9. The apparatus of claim 8, wherein the method further comprises sending a set-up message to the data network.
10. The apparatus of claim 9, wherein the method further comprises decrypting the encrypted password.
11. A computer-readable medium encoded with a method of using a virtual private network, with third party billing, the method comprising the steps of:
- a. prompting the user at a data terminal to select a destination, password, and call type;
 - b. selecting a virtual private network through the data network;
 - c. giving an encryption key to the user, and then prompting the user for a password and a user identification;
 - d. verifying the password, and providing an authorization code to the user; and
 - e. allowing the user to transfer the data through the data network to the final destination, using the authorization code.

12. The computer-readable medium of claim 11 wherein step (d) further comprises negotiating for more bandwidth for the user, and including within the authorization code a grant of additional bandwidth.

13. The computer-readable medium of claim 12 wherein step (c) further comprises encrypting the user's password, and sending the user identification and the encrypted password to the virtual private network service provider.

14. The computer-readable medium of claim 13 further comprising, after step (a), the step of sending a set-up message to the data network.

15. The computer-readable medium of claim 14 further comprising, after step (c), the step of the virtual private network service provider decrypting the encrypted password.

16. An apparatus for providing a datalink connection from a user terminal to a data network and to a virtual private network, with third party billing, comprising:

- a. means for prompting a user at the data terminal to select a destination, password, and call type;
- b. means for selecting the virtual private network through the data network;
- c. means for giving an encryption key to the user, and then prompting the user for a password and a user identification;
- d. means for verifying the password, and providing an authorization code to the user; and
- e. means for allowing the user to transfer data through the data network to a final destination, using the authorization code.

17. The apparatus of claim 16, further comprising means for negotiating for more bandwidth for the user, and including within the authorization code a grant of additional bandwidth.

18. The apparatus of claim 17, further comprising means for encrypting the user's password, and sending the user identification and the encrypted password to the virtual private network service provider.

19. The apparatus of claim 18, further comprising means for sending a set-up message to the data network.

20. The apparatus of claim 19, further comprising means for decrypting the encrypted password.

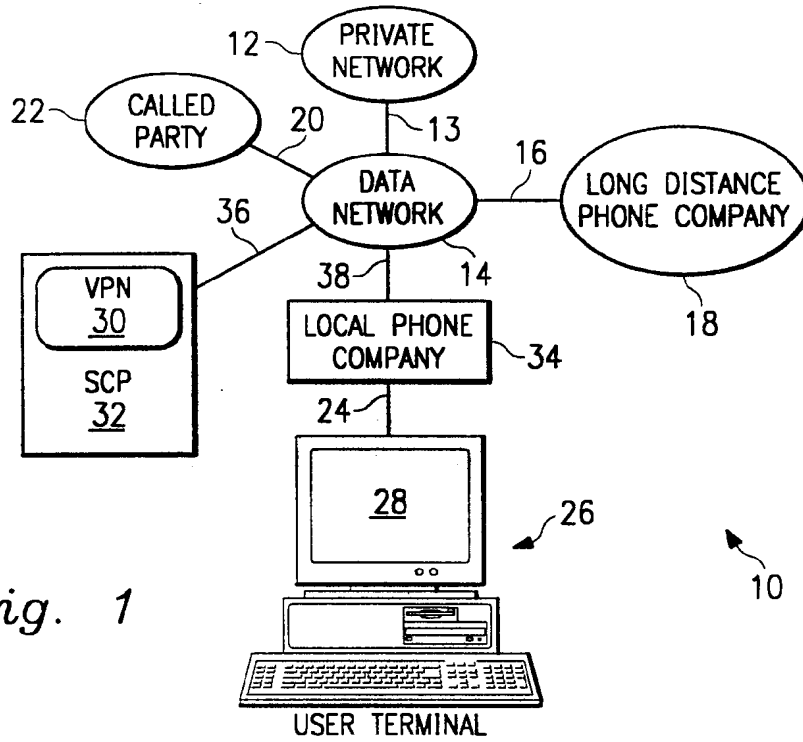


Fig. 1

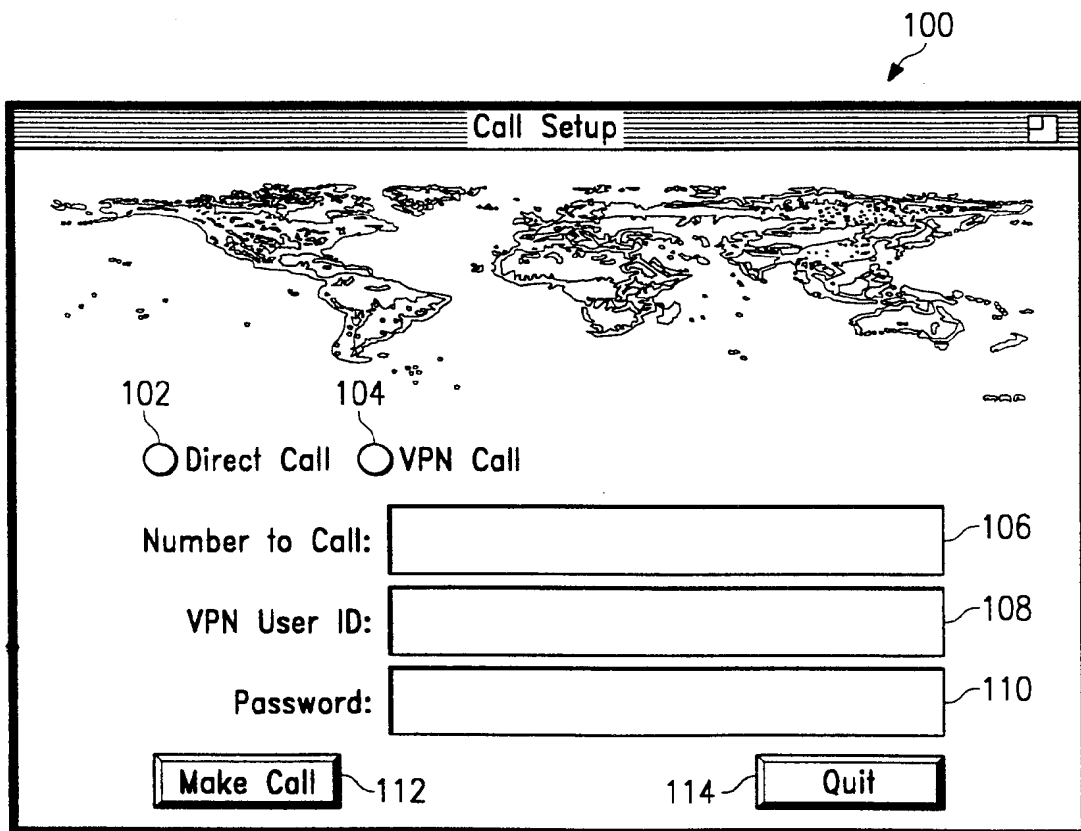


Fig. 3

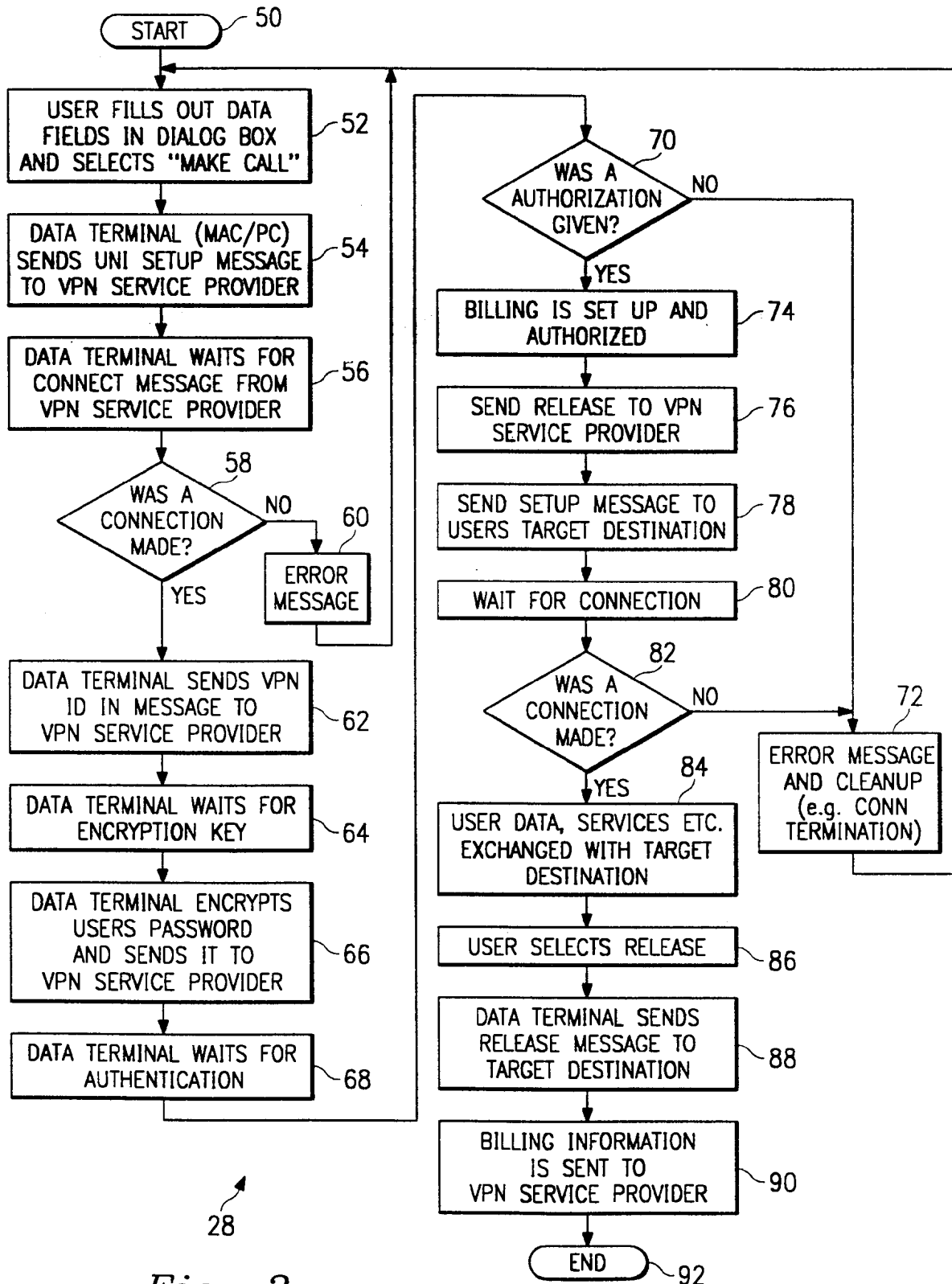


Fig. 2

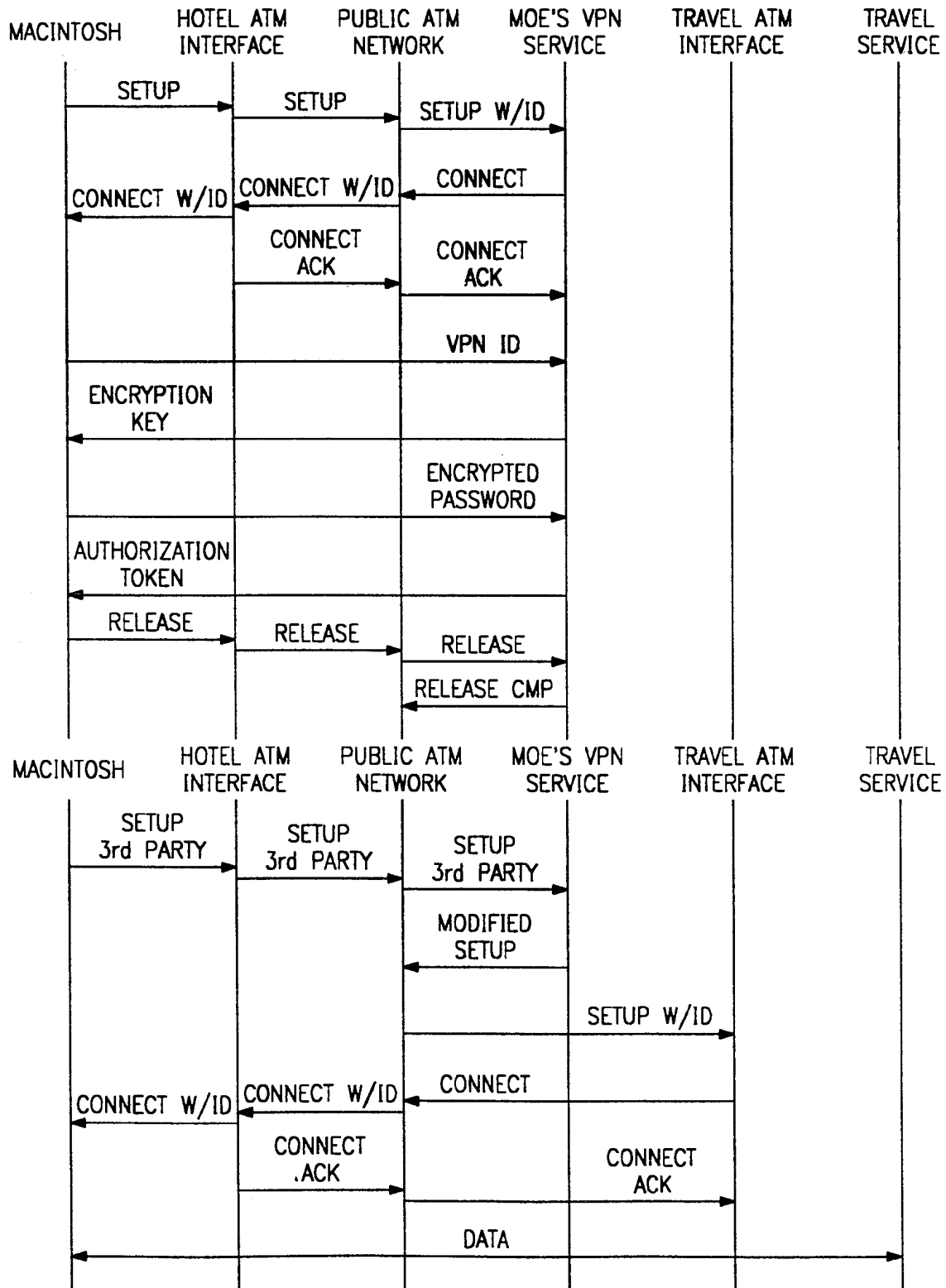


Fig. 4A

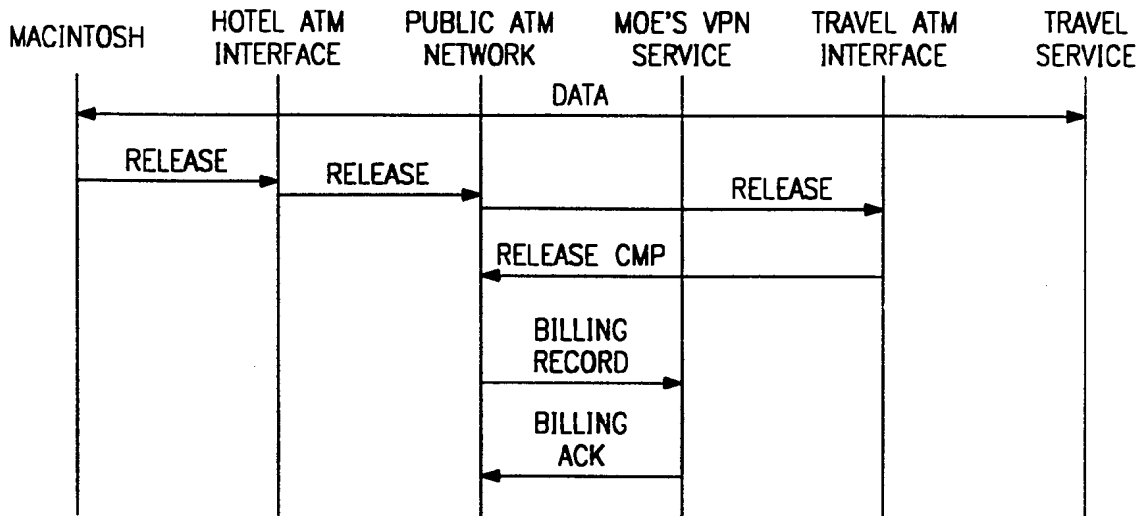


Fig. 4B

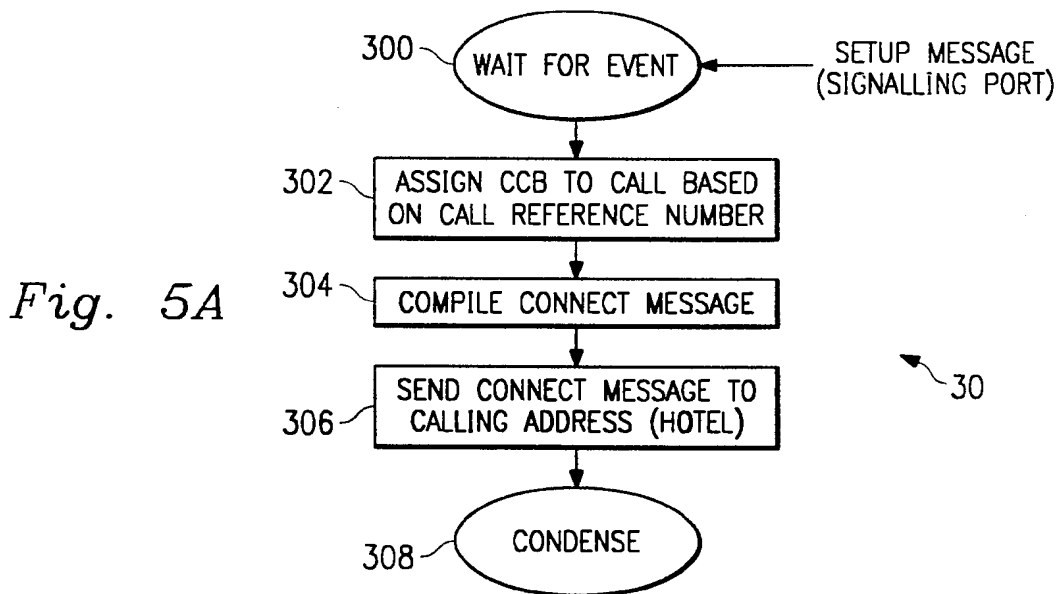


Fig. 5A

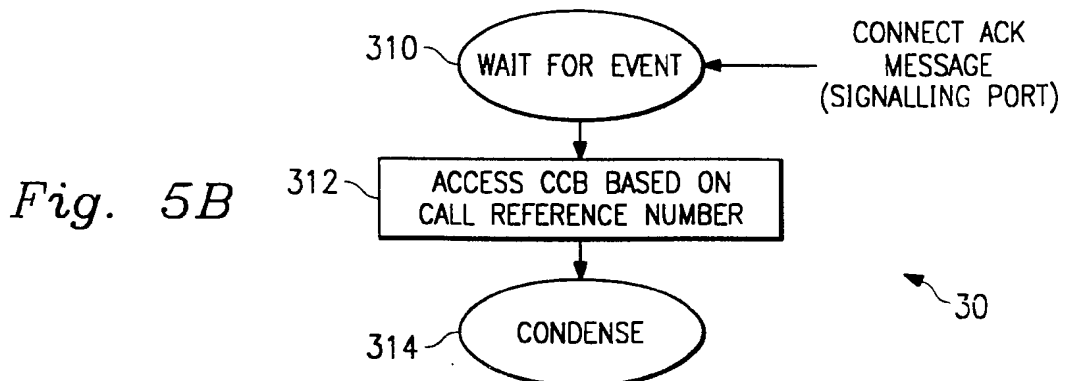


Fig. 5B

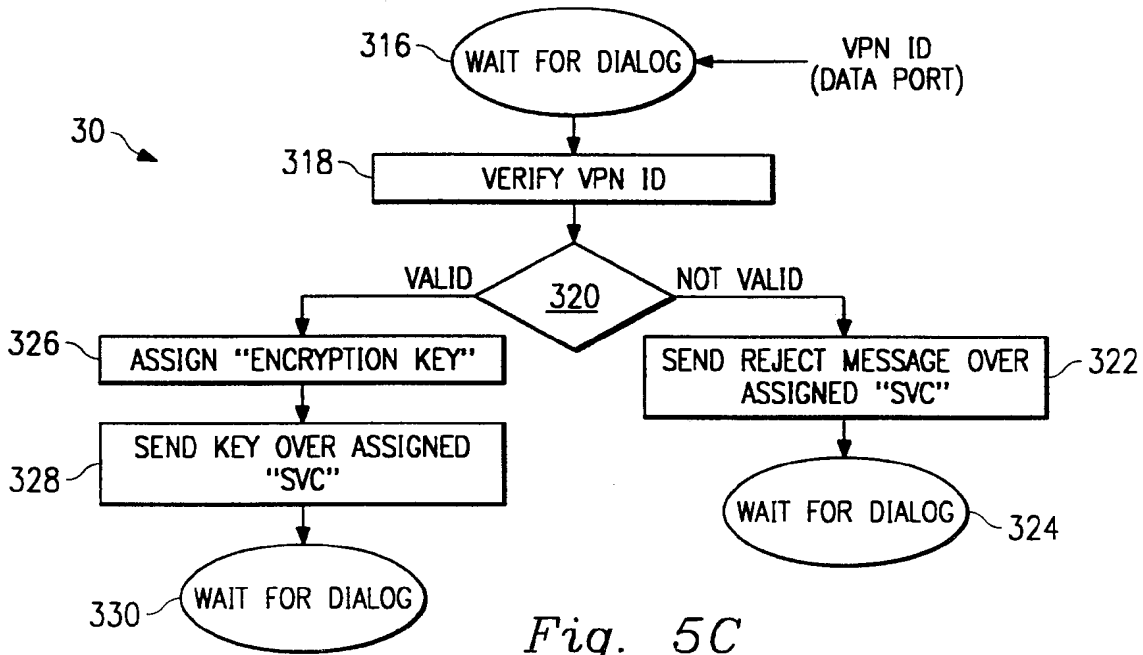


Fig. 5C

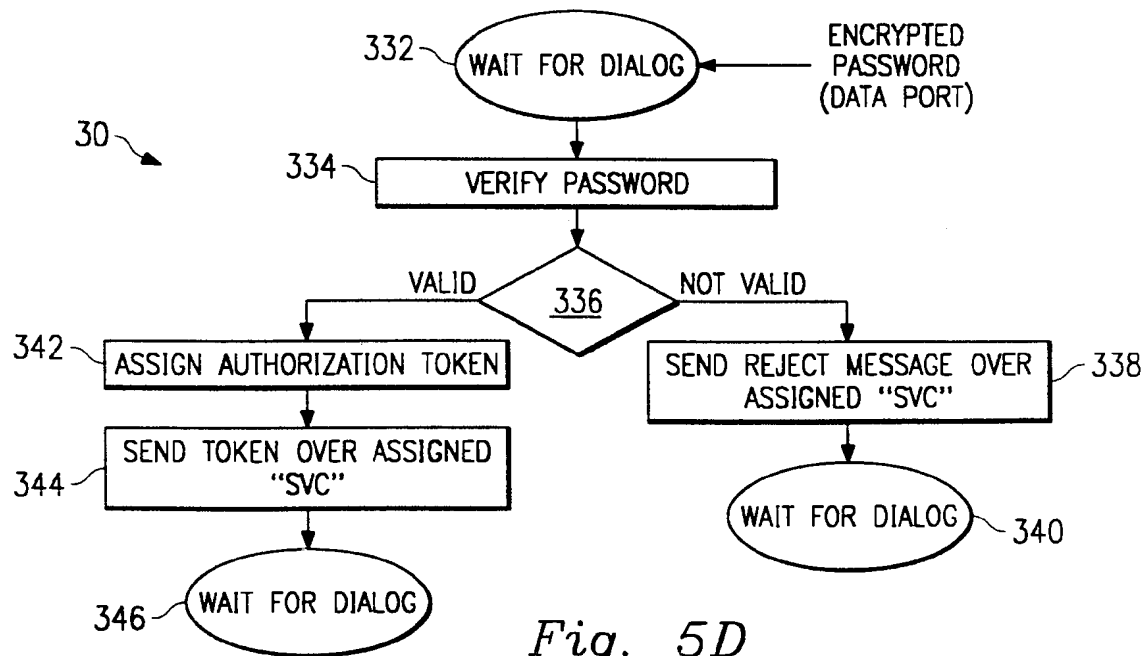
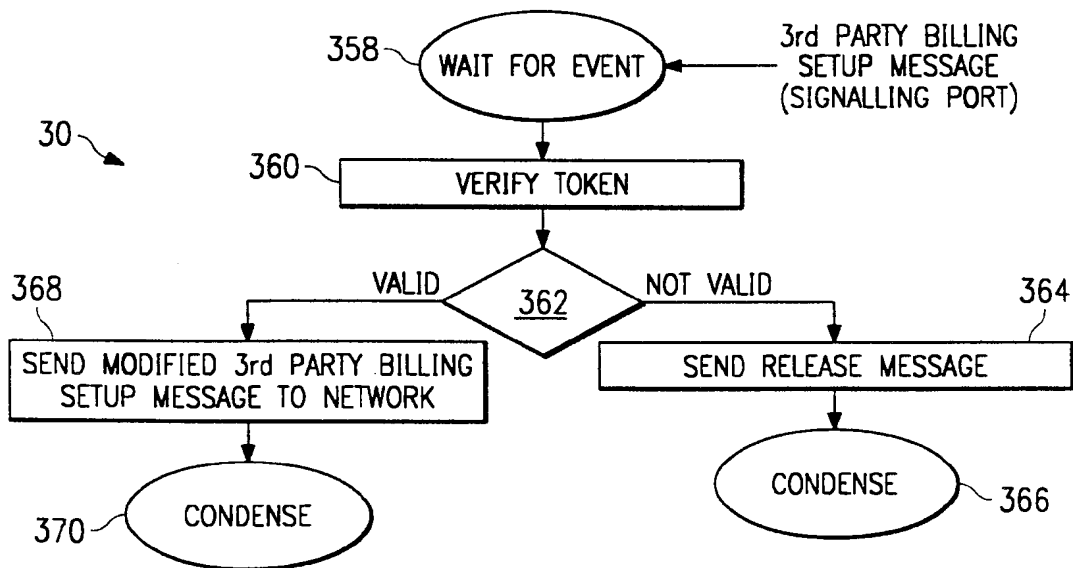
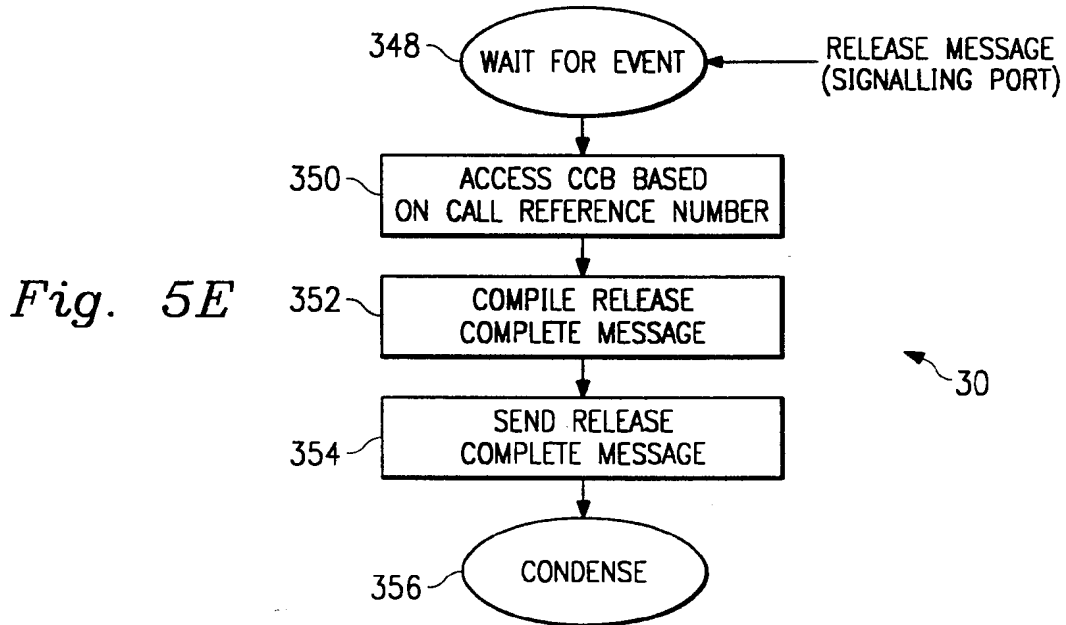


Fig. 5D



INTERNATIONAL SEARCH REPORT

International Application No PCT/IB 97/01563

A. CLASSIFICATION OF SUBJECT MATTER
 IPC 6 H04Q11/04 H04L12/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
 IPC 6 H04Q H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MUN CHOON CHAN ET AL: "AN ARCHITECTURE FOR BROADBAND VIRTUAL NETWORKS UNDER CUSTOMER CONTROL" NOMS '96 IEEE NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM , vol. 1, 15 April 1996, KYOTO, JP, pages 135-144, XP000641086 see abstract ---	1-20
A	BIC V: "VOICE PERIPHERALS IN THE INTELLIGENT NETWORK" TELECOMMUNICATIONS, vol. 28, no. 6, June 1994, page 29/30, 32, 34 XP000600293 see the whole document --- -/--	1-20

Further documents are listed in the continuation of box C. Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art. "&" document member of the same patent family
---	---

Date of the actual completion of the international search 19 March 1998	Date of mailing of the international search report 02/04/1998
---	---

Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Staessen, B
--	--

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 97/01563

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 729 256 A (NEDERLAND PTT) 28 August 1996 see abstract figures of pages 136 and 140 -----	1-20
A	CROCETTI P ET AL: "ATM VIRTUAL PRIVATE NETWORKS: ALTERNATIVES AND PERFORMANCES COMPARISONS" SUPERCOMM/ICC '94, 1 May 1994, NEW ORLEANS, US, pages 608-612, XP000438985 see abstract -----	1-20

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/IB 97/01563

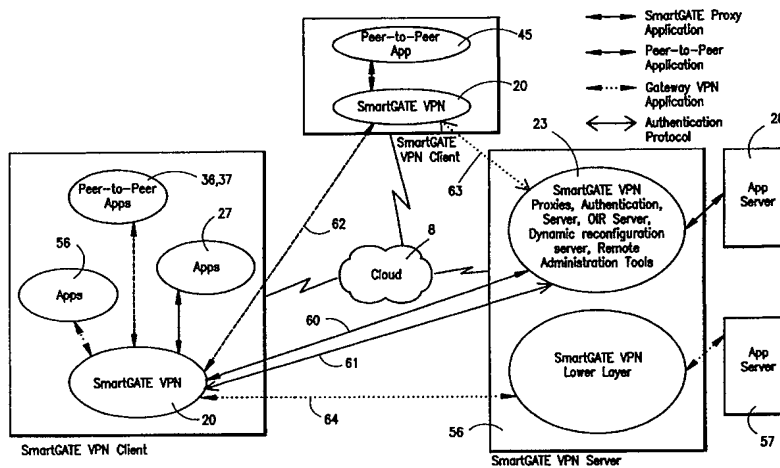
Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0729256 A	28-08-96	NL 9500339 A	01-10-96



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification ⁶ : H04L 9/00</p>	<p>A1</p>	<p>(11) International Publication Number: WO 99/11019 (43) International Publication Date: 4 March 1999 (04.03.99)</p>
<p>(21) International Application Number: PCT/US98/17198 (22) International Filing Date: 24 August 1998 (24.08.98) (30) Priority Data: 08/917,341 26 August 1997 (26.08.97) US (71) Applicant: V-ONE CORPORATION [US/US]; Suite 300, 20250 Century Boulevard, Germantown, MD 20874 (US). (72) Inventors: CHEN, James, F.; 12648 Tavilah Road, Potomac, MD 20854 (US). WANG, Jieh-Shan; 10903 Silent Wood Place, N. Potomac, MD 20878 (US). BROOK, Christopher, T.; 7308 Pomander Lane, Chevy Chase, MD 20815 (US). GARVEY, Francis; 2908 S. Buchanan Street, Arlington, VA 22206 (US). (74) Agents: URZIA, Benjamin, E. et al.; Bacon & Thomas, PLLC, 4th floor, 625 Slaters Lane, Alexandria, VA 22314 (US).</p>		<p>(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, 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).</p> <p>Published <i>With international search report.</i></p>

(54) Title: MULTI-ACCESS VIRTUAL PRIVATE NETWORK



(57) Abstract

A virtual private network for communicating between a server and clients over an open network uses an applications level encryption and mutual authentication program (20) and at least one shim (50, 53) positioned above either the layers of a client computer to intercept function calls, communicate with the server and authenticate the parties to a communication and enable the parties to the communication to establish a common session key. Where the parties to the communication are peer-to-peer applications (36, 37, 45), the intercepted function calls, request for service, or data packets include the destination address of the peer application, which is supplied to the server so that the server can authenticate the peer and enable the peer to decrypt further direct peer-to-peer communications (62).

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	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

MULTI-ACCESS VIRTUAL PRIVATE NETWORK**BACKGROUND OF THE INVENTION**1. Field of the Invention

5 This invention relates a system and method for allowing private communications over an open network, and in particular to a virtual private network which provides data encryption and mutual authentication services for both client/server and peer-to-peer applications at the applications, transport driver, and network driver levels.

10

2. Discussion of Related Art

A virtual private network (VPN) is a system for securing communications between computers over an open network such as the Internet. By securing communications between the computers, the computers are linked together as if they were on a private local area network (LAN), effectively extending the reach of the network to remote sites without the infrastructure costs of constructing a private network. As a result, physically separate LANs

15

20

can work together as if they were a single LAN, remote computers can be temporarily connected to the LAN for communications with mobile workers or telecommuting, and electronic commerce can be carried out without the risks
5 inherent in using an open network.

In general, there are two approaches to virtual private networking, illustrated in Figs. 1A and 1B. The first is to use a dedicated server 1, which may also function as a gateway to a secured network 2, to provide
10 encryption and authentication services for establishment of secured links 3 between the server 1 and multiple clients 4-6 over the open network 7, represented in Fig. 1A as a cloud, while the second is to permit private communications links 8 to be established between any two computers or
15 computer systems 9-12 on network 7, as illustrated in Fig. 1B.

The advantages of a client/server arrangement such as the one shown in Fig. 1A are that the server can handle functions requiring the majority of the computing
20 resources, increasing the number of potential clients, and that management of the network, including key management is centralized. The disadvantage of a client/server network of this type is that peer-to-peer communications links between applications on the client computers cannot utilize
25 the security and management functions provided by the server, leaving such communications unprotected. On the

other hand, the advantage of the direct peer-to-peer approach illustrated in Fig. 1B is that it permits secured links to be established between any computers capable of carrying out the required security functions, with the disadvantages being the cost of configuring each computer to carry-out encryption, authentication, and key management functions, and the lack of central control.

In both the client/server and peer-to-peer approaches, a virtual private network can in theory be based either on applications level technology or can operate at a lower level. Generally, however, peer-to-peer "tunneling" arrangements require modification of the lower layers of a computer's communications architecture, while client/server arrangements can use the applications level approach because less modification of the clients is required, and thus the two approaches are in practice mutually exclusive. The present invention, on the other hand, seeks to provide a virtual private network which utilizes a client/server approach, including centralized control of encryption, authentication, and key management functions, while at the same time enabling secured peer-to-peer communications between applications, by utilizing the server to provide authentication and session key generation functions for both client to server communications and peer-to-peer communications, providing a virtual private network capable of serving both as an extended intranet or wide area network (WAN), and as a commercial mass marketing network,

with high level mutual authentication and encryption provided for all communications.

5 In order to completely integrate the two approaches and maximize the advantage of each approach, the invention maintains the applications level infrastructure of prior client server private networking arrangements, while adding shims to lower levels in order to accommodate a variety of peer-to-peer communications applications while utilizing the applications level infrastructure for authentication and session key generation purposes. This results in the synergistic effect that not only are existing peer-to-peer tunneling schemes and applications level client server security arrangements combined, but they are combined in a way which greatly reduces implementation costs

10

15 In order to understand the present invention, it is necessary to understand a few basic concepts about computer to computer communications, including the concepts of "layers" and communications protocols, and of mutual authentication and file encryption. Further information about layers and protocols can be found in numerous sources available on the Internet, a few of which are listed at the end of this section, while a detailed description of a mutual authentication and encryption system and method suitable for use in connection with the present invention can be found in U.S. Patent No. 5,602,918, which is incorporated herein by reference. In general, the basic

20

25

communications protocols and architecture used by the present invention, as well as authentication, encryption, and key management schemes, are already well-known, and can be implemented as a matter of routine programming once the basic nature of the invention is understood. The changes made by the present invention to the conventional client server virtual private network may be thought of as, essentially, the addition of means, most conveniently implemented as shims, which add a secured mutual authentication and session key generation channel between the server and all parties to a communication, at all levels at which a communication can be carried out.

Having explained the key differences between the present invention and existing systems, the basic concepts of layers and so forth will now be briefly explained by way of background. First, the concept of "layers," "tiers," and "levels," which essential to an understanding of the invention, simply refers to libraries or sets of software routines for carrying out a group of related functions, and which can conveniently be shared or called on by different programs at a higher level to facilitate programming, avoiding duplication and maximizing computer resources. For example, the Windows NT device driver architecture is made up of three basic layers, the first of which is the Network Driver Interface Specification (NDIS 3.0) layer, the second of which is called the Transport Driver Interface (TDI) layer, and the third being the file

systems. These layers are generically referred to as the network driver layer, the transport or transport driver layer, and the applications layer.

In the Windows NT architecture, the TDI layer formats
5 data received from the various file systems or applications
into packets or datagrams for transmission to a selected
destination over the open network, while the NDIS layer
controls the device drivers that send the data, packets, or
IP datagrams, for example by converting the stream of data
10 into a waveform suitable for transmission over a telephone
line or a twisted pair cable of the type known as an
Ethernet.

By providing layers in this manner, an applications
software programmer can design an application program to
15 supply data to the TDI layer without having to re-program
any of the specific functions carried out by that layer,
and all of the transmission, verification, and other
functions required to send a message will be taken care of
the TDI layer without further involvement by the
20 applications software. In a sense, each "layer" simply
accepts data from the higher layer and formats it by adding
a header or converting the data in a manner which is
content independent, with retrieval of the data simply
involving reverse conversion or stripping of the headers,
25 the receiving software receiving the data as if the
intervening layers did not exist.

In the case of Internet communications, the most commonly used set of software routines for the transport or TDI layer, which takes care of the data formatting and addressing, is the TCP/IP protocol, in which the transport control protocol (TCP) packages the data into datagrams and provides addressing, acknowledgements, and checksum functions, and the internet protocol (IP) further packages the TCP datagrams into packets by adding additional headers used in routing the packets to a destination address. Other transport protocols which can be included in the TDI layer include the user diagram protocol (UDP), the internet control message protocol (ICMP), and non-IP based protocols such as Netbeui or IPX.

Additional "protocols" are may be used at the applications level, although these protocols have nothing to do with the present invention except that they may be included in the applications programs served by the network. Common applications level protocols which utilize the TCP/IP protocol include hypertext transfer protocol (HTTP), simple mail transfer protocol (SMTP), and file transfer protocol (FTP), all of which operate at the layer above the transport layer.

Some applications are written to directly call upon the TCP functions. However, for most applications utilizing a graphical user interface conveniently rely on a set of software routines which are considered to operate

above the TDI layer, and are known as sockets. Sockets serve as an interface between the TCP set of functions, or stack, and various applications, by providing libraries of routines which facilitate TCP function calls, so that the application simply has to refer to the socket library in order to carry out the appropriate function calls. For Windows applications, a commonly used non-proprietary socket is the Windows socket, known as Winsock, although sockets exist for other operating systems or platforms, and alternative sockets are also available for Windows, including the Winsock 2 socket currently under development.

In order to implement a virtual private network, the encryption and authentication functions must be carried out at one of the above "levels," for example by modifying the network drivers to encrypt the IP datagrams, by inserting authentication headers into the TCP/IP stacks, or by writing applications to perform these functions using the existing drivers. If possible, it is generally desirable to minimize modification of the existing levels by adding a layer to perform the desired functions, calling upon the services of the layer below, while utilizing the same function calls so that the higher layer also does not need to be modified. Such a layer is commonly referred to as a "shim."

As indicated above, the preferred approach to implementing client/server virtual private networks is to

use an applications level security system to encrypt files to be transmitted, and to then utilize existing communications layers such as Winsock, or TCP/IP directly. This is the approach taken by the commercially available access control system known as SmartGATE™, developed by V-One Corp. of Germantown, Md., which provides both encryption and mutual authentication at the applications level utilizing a dedicated server known as an authentication server and authentication client software installed at the applications level on the client computers. A description of the manner in which encryption and mutual authentication is carried out may be found in the above-cited U.S. Patent No. 5,602,918. While the principles of the invention are applicable to other client/server based virtual private networks, SmartGATE™ is used as an example because it provides the most complete range of mutual authentication and encryption services currently available.

The present invention can be implemented using the existing SmartGATE™ system, but adds mutual authentication and encryption services to lower layers by intercepting function calls or data packets and, during initialization of a communications link, establishing separate channels between the party initiating the communication and the authentication server, and between the authentication server and the party which is to share in the communication, so as to mutually authenticate the parties

with respect to the server, and so as to establish a session key which can be used for further direct communications between the parties.

5 A number of protocols exist which can be used, in total or in part, to implement the mutual authentication and encryption services at the lower layers, using the same basic authentication and encryption scheme currently implemented by SmartGATE™ at the applications level. These include, by way of example, the SOCKS protocol, which
10 places a shim between the TDI or transport layer and the applications, and the commercially available program, known as SnareNet, which operates at the network driver level and can be directly utilized in connection with the present invention.

15 On the other hand, a network level implementation such as the SKIP protocol, which operates below the TDI layer to encrypt the datagrams, and which in its description explicitly precludes the generation of session keys (see the above cited U.S. Patent No. 5,602,918), is
20 fundamentally different in concept than the present invention. Similarly, alternative implementations such as Point-to-Point Tunneling Protocol (PPTP) which involve modifying the TCP/IP stack and/or hardware to provide encryption, as opposed to inserting shims, are not utilized
25 by the preferred embodiment of the present invention, although individual aspects of the protocol could perhaps

be used, and the present system could be added to computers also configured to accept PPTP communications.

5 The SmartGATE™ system uses public key and DES encryption to provide two-way authentication and 56-bit encrypted communications between a server equipped with the SmartGATE program and client computers equipped with a separate program. Currently, SmartGATE™ operates at the highest level, or applications level, by using shared secret keys to generate a session key for use in further
10 communications between the authentication server or gateway and the client program. Since the session key depends on the secret keys at the gateway and client sides of the communication, mutual authentication is established during generation of the session key, which can then be used to
15 encrypt further communications.

When installed on a client system, the SmartGATE™ client software reads a request for communications by an applications program, such as a browser program, and then proceeds to establish its own communications link with the
20 destination server to determine if the server is an authentication server. If it is not, control of communications is relinquished, but if it is, then the security program and the server carry out a challenge/response routine in order to generate the session
25 key, and all further communications are encrypted by the security program. Although this program is placed between

the Winsock layer and the applications, it does not function as a shim, however, because it only affects communications directed to the authentication server.

Having briefly summarized the concepts used by the present invention, including the concepts of layers, protocols, and shims, and having described a specific applications level security program which is to be modified according to the present invention by adding shims in a way which enables secured authentication and session key generation channels to be set up from the lower layers, it should now be possible to understand the nature of the invention, and in particular how it integrates the two approaches to virtual private networking in a way which greatly expands the concept and yet can easily be implemented. More details will be given below, but as a final observation in this background portion of the patent specification, it should be noted that while the overall concept of the invention is in a sense very simple, it is fundamentally at odds with present approaches. For example, the literature is replete with references to conflicts between VPN standards and implementations, as exemplified by the title of an article from LAN Times On-Line, 9/96, (<http://www.wcmh.com/>), which reads *Clash Over VPN Supremacy*. Even a cursory search of the available literature indicates that the amount of information and choices available to those wishing to set up a virtual private network is overwhelming. One can choose between

Netscape Communications Secure Socket Layer, Open Market Inc.'s Secure HTTP, Microsoft's PPTP, among others. However, all of these approaches operate at a single level, and force a choice between establishing a network of the
5 type shown in Fig. 1A and a network of the type shown in Fig. 1B. Only the present invention offer the advantages of both approaches, without the inflexibility of client/server arrangements or the costs of more distributed architectures.

10 For further information on the various competing VPN protocols and systems, see also *The Development of Network Security Technologies*, Internet Smartsec, 2/97 (<http://www.smartsec.se>), which compares SmartGATE™ to other application level security systems, including PPTP,
15 SSL, and S-HTTP; *Point-To-Point Tunneling Protocol (PPTP) Frequently Asked Questions*, Microsoft Corp., date unknown, (<http://www.microsoft.com>), *Simple Key-Management for Internet Protocols (SKIP)*, Aziz et al., date unknown, (<http://skip.incog.com>), and *SOCKS Protocol Version 5, RFC*
20 *1928*, Leech et al., 3/96 (<http://andrew2.andrew.cmu.edu>) (this document describes a protocol involving a TDI shim). For more general information on security problems, Internet protocols, and sockets, see *Introduction to the Internet Protocols*, Charles L. Hedrick, Rutgers University, 1987
25 (<http://oac3.hsc.uth.tmc.edu>); *Windows Sockets - Where Necessity is the Mother of Reinvention*, Stardust

Technologies, Inc., 1996, (<http://www.stardust.com>), and
Secure Internet Connections, LAN Times, 6/17/96 (Ibid).

SUMMARY OF THE INVENTION

5 It is accordingly a principal objective of the invention to provide a client/server virtual private network which is capable not only of carrying out authenticated secure communications over an open network between an authentication server and clients, but also authenticated secure peer-to-peer communications.

10 It is also an objective the invention to provide a virtual private network that provides data encryption and mutual authentication for both client/server and peer-to-peer communications for different-types of applications, using both the applications level and lower levels of a
15 communications hierarchy.

It is a further objective of the invention to provide a client/server virtual private network which can provide both client/server and peer-to-peer encryption and authentication services for any application sharing a
20 specified socket or sockets, whether or not the application is recognized by the encryption and authentication program.

It is a still further objective of the invention to provide a client/server virtual private network which can

provide encryption and authentication services at the applications level, transport driver interface level, and network interface level, without the need for modifying either the communication driver or network driver, or any sockets utilizing the communications driver interface.

It is yet another objective of the invention to provide a virtual private network which provides encryption and authentication services for peer-to-peer communications while maintaining centralized control of key distribution and management functions.

Finally, it is also an objective of the invention to provide a virtual private network which provides encryption and authentication services for peer-to-peer communications and in which registration is carried out by a central gateway server.

These objectives of the invention are accomplished by providing a virtual private network for communicating between a server and clients over an open network and in which the clients are equipped with an applications level encryption and mutual authentication program which includes at least one shim positioned above either the socket, transport driver interface, or network interface layers of a client computers communications hierarchy, and which intercepts function calls or data packets in order to authenticate the parties to the communication by

establishing secured channels between the server and the parties to the communication, prior to establishment of the secured communications link between the parties, in order to carry out mutual authentication and session key generation functions.

More particularly, according to the principles of a preferred embodiment of the invention, client communications software is provided which, at the socket or transport driver interface levels, intercepts function calls to the socket or transport driver and directs calls to the authentication server in order to perform encryption and authentication routines, and at the network driver interface, performs encryption and authentication functions by intercepting the datagrams or data portions of the packets transmitted by the transport driver interface based on communications between the authentication server and the client. According to this aspect of the invention, a system of providing authentication and encryption services for the purpose of establishing a virtual private network includes a plurality of shims arranged to operate at different protocol levels in order to establish a common secure communications link to an authentication server.

In one especially preferred embodiment of the invention, the client software includes a Winsock shim arranged to intercept function calls to the Winsock library on a client machine and redirect initial communications

through the authentication client software to the authentication server, so that any function calls to the Winsock library of programs are intercepted by the shim and carried out by the applications level security program. In this embodiment, the client authentication software substitutes its own function calls for the original function calls in order to establish a secured communications link to the authentication server over which such functions as mutual authentication between the client and server, indirect authentication of peer applications by the now trusted server, session key generation, are carried out, as well as ancillary functions such as on-line registration (OLR), utilizing the unmodified original Winsock library and TCP/IP communications stacks.

By inserting a shim at the Winsock level, an applications level client/server based security program such as SmartGATE™ can be used to provide secure communications for any application which utilizes the Winsock library. In addition, by including analogous shims at other levels, the invention can be used to secure virtually any communications application, including those which by-pass the TDI layer and communicate directly with the network driver level.

Instead of the current array of mutually exclusive alternative methods and systems of establishing secured communications over an open network, the invention thus

provides a single integrated method and system capable of carrying out both client/server communications and peer-to-peer communications between a wide variety of communications applications regardless of whether the applications use a socket or even commonly accepted internet protocols, with complete mutual authentication and encryption of data files at all levels and between all parties to the network.

It will be appreciated that the term "virtual private network" is not to be taken as limiting, and that the principles of the invention can be applied to any remote access schemes which utilize the Internet or other relatively insecure networks to provide access for remote users, corporate intranets, and electronic commerce.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1A is a schematic diagram of a client/server virtual private network.

Fig. 1B is a schematic diagram of an alternative virtual private network based on peer-to-peer communications.

Fig. 2 is a functional block diagram showing the operation of an applications level security program in a conventional communications network hierarchy.

Fig. 3 is a functional block diagram showing the communications network hierarchy of Fig. 1, modified to provide a second layer of service in accordance with the principles of a preferred embodiment of the invention.

5 Fig. 4 is a functional block diagram showing the communications network hierarchy of Fig. 2, modified to provide a third layer of service in accordance with the principles of the preferred embodiment.

10 Fig. 5 is a functional block diagram showing the communication network hierarchy of Fig. 3, modified to provide a fourth layer of service in accordance with the principles of the preferred embodiment.

15 Fig. 6 is a schematic diagram of a virtual private network utilizing the principles of the preferred embodiment of the invention.

Fig. 7 is a flowchart illustrating a method of implementing the system of the preferred embodiment.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

20 Fig. 2 illustrates the operation of a client authentication program which is utilized in the present invention. An example of such a program is the SmartGATE™ program discussed briefly above, although other

applications level security programs, whether or not token based, could be modified in a manner similar to that discussed in the following description. The illustrated hierarchy is the Windows NT architecture, although versions of SmartGATE™ exist for other architectures, and the invention could easily be adapted for use with any version of SmartGATE™, including UNIX and MacIntosh versions, as well as for use with applications level security programs designed for communications architectures other than those supported by SmartGATE™. Conversely, it is intended that the present invention can be used with authentication and encryption schemes other than that used by SmartGATE™ and disclosed in U.S. Patent No. 5,602,918. For purposes of convenience, therefore, the software represented by SmartGATE™ is simply referred to as client authentication software.

In addition, it noted that the client computer architectures illustrated in Figs. 3-6, which are modified versions of the architecture of Fig. 2, is to be used with an overall network layout such as the one illustrated in Fig. 6, which includes an authentication server that may be a SmartGATE™ server, or another server depending on the client authentication software. The invention is not merely the addition of shims to the client software, but involves the manner in which the shims are used in the establishment of the authentications and key generation links to the server.

Turning to Fig. 2, which provides background for the description of the invention illustrated in Figs. 3-6, the client authentication software 20 is situated above the boundary of the transport or TDI layer 21 and is designed to utilize a socket 22, such as Winsock, to carry out communications with the authentication server 23 shown in Fig. 6 by means of a transport protocol such as TCP/IP, UDP, or the like, which in turn supply datagrams or packets to a hardware driver layer 24, such as NDIS 3.0, of a network or modem connection 25.

In operation, the client authentication software 20 intercepts interconnect calls 26 from client authentication software supported applications 27 and, if the calls are directed to the authentication server 23, or to a server 28 situated on a secured network whose access is controlled by the authentication server, establishes a secured communications link to the server by executing appropriate function calls 29 to the socket library, which in turn transmits function calls 30 to the TDI layer, causing the TDI layer to form datagrams or packets 31. Datagrams or packets 31 are then formatted over packaged for transmission by the hardware drivers 24 and sent to the communications network in the form of Ethernet packets or analog signals 32 containing the original datagrams from the TDI layer. Once the secured communications link has been established, client authentication software 20 encrypts all further data communications 34 from

applications 27, which are indicated by dashed lines, before handing them off to the next lower layer in the form of encrypted files 35. The dashed lines are shown in Fig. 2 as extending only to the TDI layer 21, because the datagrams formed by the TDI layer are indistinguishable as to content, but it is to be understood that datagrams or packets 31 carry both the communications used to establish the secure channel, and the encrypted files subsequently sent therethrough.

10 Finally, in the case of SmartGATE™, the authentication client software utilizes either a smart card or secured file to supply the secret keys used during authentication to generate a session key for encryption of further communications, and also to carry out certain other encryption and authentication functions, although it is of course within the scope of the invention to use key distribution and authentication methods which do not rely on smartcards or tokens, and the tokens are not involved in any of the basic communications functions of the client authentication software 20.

25 In addition to the applications 27 which communicate with the server via the authentication/encryption software 20, a typical system will have a number of additional software applications 36 and 37 capable of carrying out communications over the open network, but which the authentication client software is not configured to handle,

and which are not specifically adapted or intended to carry out communications with the authentication server. These are referred to herein as peer-to-peer applications, and can include applications which use the same sockets as the authentication client software, applications which directly call upon a transport driver interface stack, whether using the same protocol as the authentication client software or another protocol, all of which are intended to be represented by the TDI layer, and applications which are written to call directly upon the hardware drivers. These peer-to-peer applications may have their own encryption and authentication capabilities, but cannot utilize the services of the authentication server or client software, and therefore the function calls made by the applications and the files transmitted are indicated by separate reference numerals 40-43.

It will be appreciated by those skilled in the art that lower layer application programs which generate packets in forms other than those represented by the TDI layer are also possible, and should be considered within the scope of the invention, but at present virtually all open network applications use at least one of the TDI protocols, and thus while these programs may interact directly with the network driver layer, and require a network driver layer shim, as will be discussed below, are illustrated for purposes of convenience as part of the TDI layer applications.

Turning now to a preferred embodiment of the invention, the arrangement shown in Fig. 3 modifies the arrangement of Fig. 2 by adding a socket shim 50 between the socket 22 utilized by the authentication client software 20, the peer-to-peer applications 36 which also
5 utilize the socket 20, and the authentication client software itself. The shim 50 operates by hooking or intercepting call initiation function calls 40 made to the socket and, in response thereto, having the authentication
10 client software initiate communications with the authentication server 23, shown in Fig. 6, in order to carry out the authentication protocol, as will be discussed in more detail below. Shim 50 also causes files 41
15 intended for the TDI layer to be diverted to the authentication software for encryption based on the session keys generated during the initial communications with the authentication server, and transmission as encrypted files
20 51 addressed to the peer application, also shown in Fig. 6, which could also be an application on the application server 28.

Since the basic authentication client software is designed to send all communications directly to the authentication server, while the peer-to-peer applications are designed only to communicate with "peers" 45 and not
25 with the authentication server, the principal function of shim 50 is to arrange for the destination of address of the communication to be supplied to both the authentication

client software and to authentication server, even though
the peer application assumes that it is communicating only
with the peer application. This function permits session
key encrypted communications to be forwarded directly to
5 the peer application, as illustrated in Fig. 6, while the
latter function provides the authentication server with the
client address so that the authentication server can
establish a secured and authenticated link with the peer
application, via authentication client software on the peer
10 computer, and transmit the session key to the peer
application or at least enable the peer application to
recreate the session so that it can decrypt the encrypted
files received directly from the client application.

Thus, while it is appreciated that the use of socket
15 shims is well-known, as mentioned above, the socket shim
shown in Fig. 2 has the unique function of enabling direct
peer-to-peer communications with mediation by the
authentication server, permitting the highest level of
authentication service and collateral functions. In
20 addition, because of the mediation by the key server, the
peer applications do not need to have a shared secret key,
allowing centralized key management, with only the
authentication server having access to all of the client's
secret keys.

25 Figs. 4 shows the variation of the client
authentication software 20 in which a TDI shim 52 similar

in function to the socket shim 50 is provided above the TDI layer. Like the socket shim, implementation of the TDI shim essentially simply involves diverting certain information to the client software in order to establish a communications link with the authentication server, and subsequently perform encryption to obtain encrypted files for transmission directly through the TDI layer in the usual manner. As with the socket shim, TDI shims are not new and can be implemented in known manner, by intercepting TDI service requests, but with the difference from prior TDI shims that the TDI shim works with the authentication software and authentication server to authenticate communications and generate a session key.

Finally, as shown in Fig. 5, a further layer of authentication and encryption may be added by adding a network driver shim 55, either to the arrangement shown in Fig. 3 without the TDI shim, in combination with the TDI shim shown in Fig. 4, or in combination with the TDI shim of Fig. 4 but not the socket shim, to provide for authentication of communications at the network driver layer. At this layer, the shim 55 intercepts IP packets from applications 56, but instead of referring back to the applications level routine, checks the destination address (which can be in TCP format, UDP format, and so forth), establishes a session key by communications with the authentication server, converts the session key into a format which can be used to encrypt the IP packet, and

sends the IP packet towards the destination, all by carrying out the necessary operations at the network driver level, in a manner similar to that utilized by the above-mentioned SnareNet software program, but with the difference that the authenticating communications link and key generation is carried out by packets addressed to a corresponding layer 56 of the authentication server, which may be further connected to an applications server 57.

It will be noted that since the IP packets are not distinguishable by content, the network driver layer shim could be used as an additional level of security, rather than as an alternative to applications level encryption, with the encrypted files generated by software 20 being further encrypted by shim 55 before transmission to the authentication server or associated gateway.

The overall system utilizing the authentication client software illustrated in Figs. 3-5 is schematically illustrated in Fig. 6. The principal components of the overall system are the client computers containing software of the type illustrated in Figs. 2-5, including client authentication software 20 and shims 50, 53, and/or 55, and applications with communications capabilities (represented by applications 27, 36, 37, and 56 on one client, and application 45 on the other). For purposes of illustration, the client of Figs. 6 is thus depicted as including applications for communicating at the highest

levels, such as the SmartGATE™ proxy application, applications for communicating at the network driver level with corresponding applications connected to the lower layer of the authentication server, and peer-to-peer applications with no capability of communicating with SmartGATE™, but which use sockets or TDI protocols recognized by the shims.

In the case of the SmartGATE™ proxy application, communications are established in the same manner as in the currently available version of the SmartGATE™ authentication client software, and as described in U.S. Patent No. 5,602,918, the communications link being indicated by arrows 60 and 61, with arrow 60 representing the client/server response channel used to authenticate the parties and generate the session key.

In the case of a peer-to-peer application, in which the clients wish to communicate over a direct link 62, the invention provides for the function calls establishing the communications to be intercepted and the initialization procedure routed through channel 61 to the authentication server 23. Server 23 then opens a secured channel 63 to the authentication client software 20 associated with peer application 45 by performing the same mutual authentication procedure performed for the purpose of establishing channel 63, and once the channel is established with its own session key, transmits information using the channel 63

session key which allows the client to recreate the channel
60 session key for use in decrypting communications sent
over channel 62. Alternatively, after establishing channel
63, the channel 60 session key could be used to transmit
5 back to the original sending party information necessary to
recreate the channel 63 session key. In either case, the
authentication server is thus used to establish a fully
authenticated "tunnel" between the peer applications
without the need to modify any of the sockets, TDI
10 protocols, or hardware drivers on either of the client
computers. While the transmitting peer application has no
way of directly authenticating the receiving peer, only a
receiving peer authenticated by the authentication server
will be able to generate the necessary session keys, and
15 thus each of the parties to the communication is
effectively authenticated.

For the lower layer application 56, a similar protocol
may be employed, in which the attempted communication
between lower layer applications is intercepted, and the
20 communications link to the authentication server is used to
generate a session key, which is then used to encrypt the
packets or datagrams being sent. In this case, the
destination must be the lower layer of the authentication
server, and thus the communications link is indicated by a
25 separate channel 67.

Finally, the procedures associated with the network illustrated in Fig. 6 are summarized in the flowchart of Fig. 7. For communications directly with the applications level portion of the server 23, steps 100-103 are used, while for peer-to-peer communications, steps 104-109 are used, and for network driver level communications, steps 110-114 are used.

In particular, step 100 by which the applications level authentication program 20 illustrated in Figs. 3-5 receives a call initiation request, either directly from a supported applications program 27 or from a programs 36 and 37 via one of the shims 50 and 53, step 101 is step by which the program 20 addresses the authentication server, step 102 is the step by which the client and server are mutually authenticated and the session keys generated using, for example, the procedure described in U.S. Patent No. 5,602,918, and step 103 is the step by which program 20 encrypts further communications received directly or via shims 50 and 53 from the applications programs 27, 36, and 37.

For peer-to-peer communications, step 105, which is part of step 100, is the step by which the peer address is supplied to program 20, steps 106 and 107 are identical to steps 101 and 102, step 108 is the step by which communications channel 63 shown in Figure 6 is established, step 109 is the step by which the destination computer

authenticated by the server is enabled to decrypt communications received over channel 62, and step 110 is the step by which program 20 encrypts the communications. It will of course be appreciated that these steps represent only a summary of the steps involved in carrying out the present invention, and that further steps will be apparent to those skilled in the art based on the above description of the apparatus and software portions of the preferred embodiment of the invention.

10 Having thus described various preferred embodiments of the invention, those skilled in the art will appreciate that variations and modifications of the preferred embodiment may be made without departing from the scope of the invention. It is accordingly intended that the invention not be limited by the above description or
15 accompanying drawings, but that it be defined solely in accordance with the appended claims.

I claim:

1. Apparatus for carrying out communications over a multi-tier virtual private network, said network including a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network, comprising:

means for intercepting function calls and requests for service sent by an applications program on one of said client computers to a lower level set of communications drivers; and

means for causing an applications level authentication and encryption program in said one of said client computers to communicate with the server, generate said session key, and encrypt files sent by the applications program before transmittal over said open network.

2. Apparatus as claimed in claim 1, further comprising means for intercepting files packaged by a transport driver interface layer to form packets and encrypting the packets using a session key generated during communications with a lower layer of the server.

3. A method as claimed in claim 1, further comprising means for intercepting a destination address during initialization of communications between said one of said

client computers and a second of said client computers on said virtual private network;

means for causing said applications level authentication and encryption program to communicate with the server to carry out functions a.) and b.);

means for transmitting said destination address to said server;

means for causing said server to carry-out functions a.) and b.) with respect to the second of said two client computers;

means for enabling said second of said two client computers to recreate the session key;

means for causing said authentication software to encrypt files to be sent to the destination address using the session key; and

means for transmitting the encrypted files directly to the destination address.

4. Apparatus as claimed in claim 3, wherein said means for intercepting the destination address is carried out by a shim positioned between a peer-to-peer applications program and a layer of a communications driver architecture of said one of the two client computers.

5. A multi-tier virtual private network, comprising:

a server and a plurality of client computers, the server and client computers each including means for

transmitting data to and receiving data from an open network,

wherein said means for transmitting data to and receiving data from the open network includes, in any client computer initiating communications with the server:

applications level encryption and authentication software arranged to communicate with the server in order to: a.) mutually authenticate the server and the client computer initiating communications with the server and b.) generate a session key for use by the client computer initiating communications to encrypt files;

at least one lower level set of communications drivers;

and a shim arranged to intercept function calls and requests for service sent by an applications program to the lower level set of communications drivers in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files sent by the applications program before transmittal over said open network.

6. A multi-tier virtual private network as claimed in claim 5, wherein said lower level set of communications drivers includes a network driver layer, a transport driver

interface layer arranged to package applications files as packets capable of being routed over the open network and supply the packets to the network driver layer for transmission to the open network, and an applications socket for facilitating service requests by said applications program to the transport driver interface layer, and wherein said shim is a socket shim positioned between the applications program and the socket to intercept function calls to the socket in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files sent by the applications program before the files are packaged by the transport driver interface layer.

7. A multi-tier virtual private network as claimed in claim 6, wherein said applications program is a peer-to-peer communications program, and wherein a peer application destination address, included in said function calls to the socket, is diverted by the socket shim and wherein a destination address including said intercepted function calls is supplied to the server during communications with the server, causing the service to establish a communications link with a peer application, mutually authenticate the peer application, and enable the peer application to reconstruct the session key in order to receive encrypted files sent by the peer-to-peer communications program over the open network.

8. A multi-tier virtual private network as claimed in claim 6, further including a transport driver interface shim positioned between the transport driver interface layer and a second applications program, for intercepting requests from the second applications program for service by the transport driver interface layer in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files sent by the applications program before the files are packaged by the transport driver interface layer.

9. A multi-tier virtual private network as claimed in claim 8, further comprising a network driver layer shim positioned between the network driver layer and the transport driver interface layer and arranged to intercept files packaged by the transport driver interface layer and encrypt the files using a session key generated during communications with a lower layer of the server.

10. A multi-tier virtual private network as claimed in claim 5, wherein said lower level set of communications drivers includes a network driver layer, and a transport driver interface layer arranged to package applications files as packets capable of being routed over the open network and supply the packets to the network driver layer for transmission to the open network, and wherein said shim is a transport driver interface layer shim positioned

between the applications program and the transport driver interface layer to intercept service requests by the applications program to the transport driver interface layer in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files sent by the applications program before the files are packaged by the transport driver interface layer.

11. A multi-tier virtual private network as claimed in claim 10, wherein said applications program is a peer-to-peer communications program, and wherein a peer application destination address, included in said intercepted requests for service, is diverted by the transport driver interface layer shim and supplied to the server during communications with the server, causing the service to establish a communications link with a peer application, mutually authenticate the peer application, and enable the peer application to reconstruct the session key in order to receive encrypted files sent by the peer-to-peer communications program over the open network.

12. A multi-tier virtual private network as claimed in claim 10, further comprising a network driver layer shim positioned between the network driver layer and the transport driver interface layer and arranged to intercept files packaged by the transport driver interface layer and

encrypt the files using a session key generated during communications with a lower layer of the server.

13. A multi-tier virtual private network, comprising:

a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network,

wherein said means for transmitting data to and receiving data from the open network includes, in any client computer initiating communications with the server:

applications level encryption and authentication software arranged to communicate with the server in order to: a.) mutually authenticate the server and the client computer initiating communications with the server and b.) generate a session key for use by the client computer initiating communications to encrypt files; and

at least one lower level set of communications drivers,

wherein said lower level set of communications drivers includes a network driver layer, a transport driver interface layer arranged to package applications files as packets capable of being routed over the open network and supply the packets to the network driver layer for transmission to the open network, and a

network driver layer shim positioned between the transport driver interface layer and the network driver layer and arranged to intercept files packaged by the transport driver interface layer and encrypt the files using a session key generated during communications with a lower layer of the server.

14. A multi-tier virtual private network, comprising:

a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network,

wherein said means for transmitting data to and receiving data from the open network includes, in any client computer initiating communications with the server:

applications level encryption and authentication software arranged to communicate with the server in order to: a.) mutually authenticate the server and the client computer initiating communications with the server and b.) generate a session key for use by the client computer initiating communications to encrypt files; and

further comprising means for securing peer-to-peer communications between applications on two of said client computers, said peer-to-peer communications securing means comprising:

means for intercepting a destination address during initialization of communications by a first of said two client computers;

means for causing said authentication software to communicate with the server to carry out functions a.) and b.);

means for transmitting said destination address to said server;

means for causing said server to carry-out functions a.) and b.) with respect to the second of said two client computers;

means for enabling said second of said two client computers to recreate the session key;

means for causing said authentication software to encrypt files to be sent to the destination address using the session key;

means for transmitting the encrypted files directly to the destination address.

15. A multi-tier virtual private network as claimed in claim 14, wherein said means for intercepting the destination address comprises a shim positioned between the peer-to-peer applications program and a layer of a communications driver architecture of said first of the two client computers.

16. A multi-tier virtual private network as claimed in claim 5, wherein said shim is positioned above a socket,

the socket being positioned above a transport driver layer of said communications driver architecture.

17. A multi-tier virtual private network as claimed in claim 5, wherein said shim is positioned above a transport driver layer of said communications driver architecture.

18. Computer software for installation on a client computer of a multi-tier virtual private network, said network including a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network,

wherein said computer software includes:

 applications level encryption and authentication software arranged to communicate with the server in order to: a.) mutually authenticate the server and the client computer initiating communications with the server and b.) generate a session key for use by the client computer initiating communications to encrypt files;

 and a shim arranged to intercept function calls and requests for service sent by an applications program to a lower level set of communications drivers in order to cause the applications level authentication and encryption program to communicate with the server, generate

said session key, and encrypt files sent by the applications program before transmittal over said open network.

19. Computer software as claimed in claim 18, wherein said lower level set of communications drivers includes a network driver layer, a transport driver interface layer arranged to package applications files as packets capable of being routed over the open network and supply the packets to the network driver layer for transmission to the open network, and an applications socket for facilitating service requests by said applications program to the transport driver interface layer, and wherein said shim is a socket shim positioned between the applications program and the socket to intercept function calls to the socket in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files sent by the applications program before the files are packaged by the transport driver interface layer.

20. Computer software as claimed in claim 19, wherein said applications program is a peer-to-peer communications program, and wherein a peer application destination address, included in said function calls to the socket, is diverted by the socket shim and wherein a destination address including said intercepted function calls is supplied to the server during communications with the

server, causing the service to establish a communications link with a peer application, mutually authenticate the peer application, and enable the peer application to reconstruct the session key in order to receive encrypted files sent by the peer-to-peer communications program over the open network.

21. Computer software as claimed in claim 19, further including a transport driver interface shim positioned between the transport driver interface layer and a second applications program, for intercepting requests from the second applications program for service by the transport driver interface layer in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files sent by the applications program before the files are packaged by the transport driver interface layer.

22. Computer software as claimed in claim 21, further comprising a network driver layer shim positioned between the network driver layer and the transport driver interface layer and arranged to intercept files packaged by the transport driver interface layer and encrypt the files using a session key generated during communications with a lower layer of the server.

23. Computer software as claimed in claim 18, wherein said lower level set of communications drivers includes a

network driver layer, and a transport driver interface layer arranged to package applications files as packets capable of being routed over the open network and supply the packets to the network driver layer for transmission to the open network, and wherein said shim is a transport driver interface layer shim positioned between the applications program and the transport driver interface layer to intercept service requests by the applications program to the transport driver interface layer in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files sent by the applications program before the files are packaged by the transport driver interface layer.

24. Computer software as claimed in claim 23, wherein said applications program is a peer-to-peer communications program, and wherein a peer application destination address, included in said intercepted requests for service, is diverted by the transport driver interface layer shim and supplied to the server during communications with the server, causing the service to establish a communications link with a peer application, mutually authenticate the peer application, and enable the peer application to reconstruct the session key in order to receive encrypted files sent by the peer-to-peer communications program over the open network.

25. Computer software as claimed in claim 23, further comprising a network driver layer shim positioned between the network driver layer and the transport driver interface layer and arranged to intercept files packaged by the transport driver interface layer and encrypt the files using a session key generated during communications with a lower layer of the server.

26. Computer software for installation on a client computer of a multi-tier virtual private network, said network including a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network,

wherein said computer software includes:

applications level encryption and authentication software arranged to communicate with the server in order to: a.) mutually authenticate the server and the client computer initiating communications with the server and b.) generate a session key for use by the client computer initiating communications to encrypt files; and

at least one lower level set of communications drivers,

wherein said lower level set of communications drivers includes a network driver layer, a transport driver interface layer

arranged to package applications files as packets capable of being routed over the open network and supply the packets to the network driver layer for transmission to the open network, and a network driver layer shim positioned between the transport driver interface layer and the network driver layer and arranged to intercept files packaged by the transport driver interface layer and encrypt the files using a session key generated during communications with a lower layer of the server.

27. Computer software for installation on a client computer of a multi-tier virtual private network, said network including a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network,

wherein said computer software includes:

applications level encryption and authentication software arranged to communicate with the server in order to: a.) mutually authenticate the server and the client computer initiating communications with the server and b.) generate a session key for use by the client computer initiating communications to encrypt files; and

further comprising means for securing peer-to-peer communications between applications on two of said client

computers, said peer-to-peer communications securing means comprising:

means for intercepting a destination address during initialization of communications by a first of said two client computers;

means for causing said authentication software to communicate with the server to carry out functions a.) and b.);

means for transmitting said destination address to said server;

means for causing said server to carry-out functions a.) and b.) with respect to the second of said two client computers;

means for enabling said second of said two client computers to recreate the session key;

means for causing said authentication software to encrypt files to be sent to the destination address using the session key;

means for transmitting the encrypted files directly to the destination address.

28. Computer software as claimed in claim 27, wherein said means for intercepting the destination address comprises a shim positioned between the peer-to-peer applications program and a layer of a communications driver architecture of said first of the two client computers.

29. Computer software as claimed in claim 27, wherein said shim is positioned above a socket, the socket being positioned above a transport driver layer of said communications driver architecture.

30. Computer software as claimed in claim 27, wherein said shim is positioned above a transport driver layer of said communications driver architecture.

31. A method of carrying out communications over a multi-tier virtual private network, said network including a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network, comprising the steps of:

intercepting function calls and requests for service sent by an applications program in one of said client computers to a lower level set of communications drivers;

causing an applications level authentication and encryption program said one of said client computers to communicate with the server, generate said session key, and encrypt files sent by the applications program before transmittal over said open network.

32. A method as claimed in claim 31, further comprising the step of intercepting files packaged by a transport driver interface layer to form packets and encrypting the

packets using a session key generated during communications with a lower layer of the server.

33. A method as claimed in claim 31, further comprising the step of intercepting a destination address during initialization of communications between said one of said client computers and a second of said client computers on said virtual private network;

causing said applications level authentication and encryption program to communicate with the server to carry out functions a.) and b.);

transmitting said destination address to said server;

causing said server to carry-out functions a.) and b.) with respect to the second of said two client computers;

enabling said second of said two client computers to recreate the session key;

causing said authentication software to encrypt files to be sent to the destination address using the session key; and

transmitting the encrypted files directly to the destination address.

34. A method as claimed in claim 33, wherein said step of intercepting the destination address is carried out by a shim positioned between a peer-to-peer applications program

and a layer of a communications driver architecture of said one of the two client computers.

Client/Server VPN

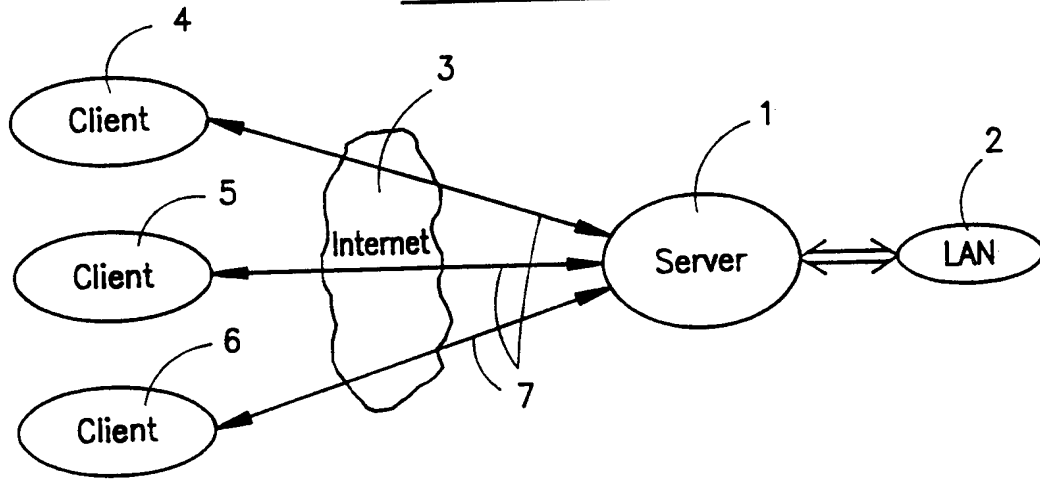


FIG. 1A
(PRIOR ART)

Peer-to-Peer Tunneling

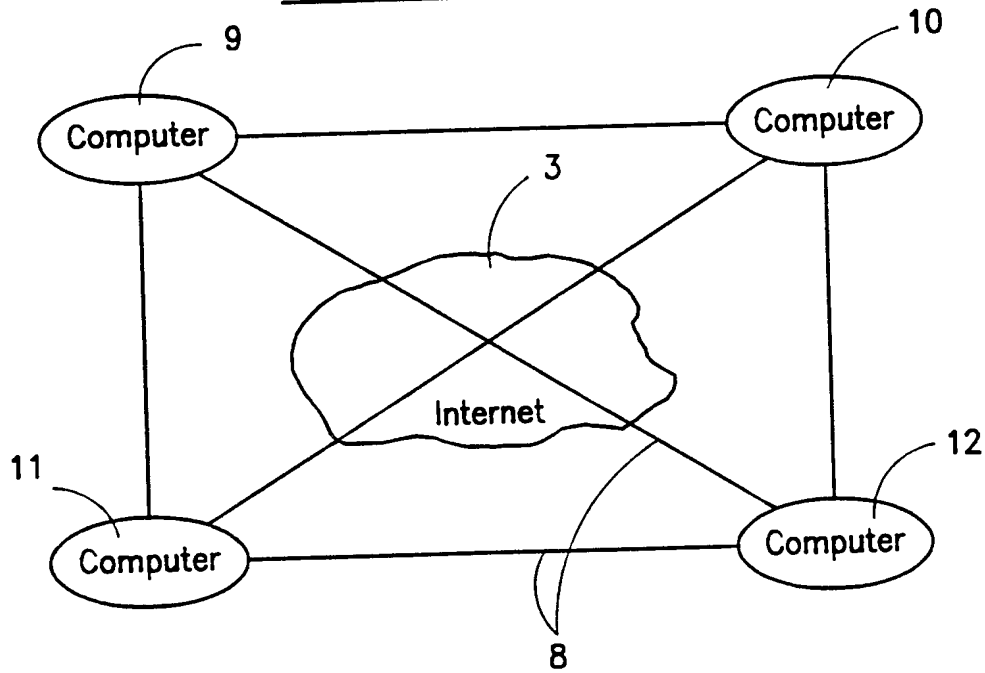


FIG. 1B
(PRIOR ART)

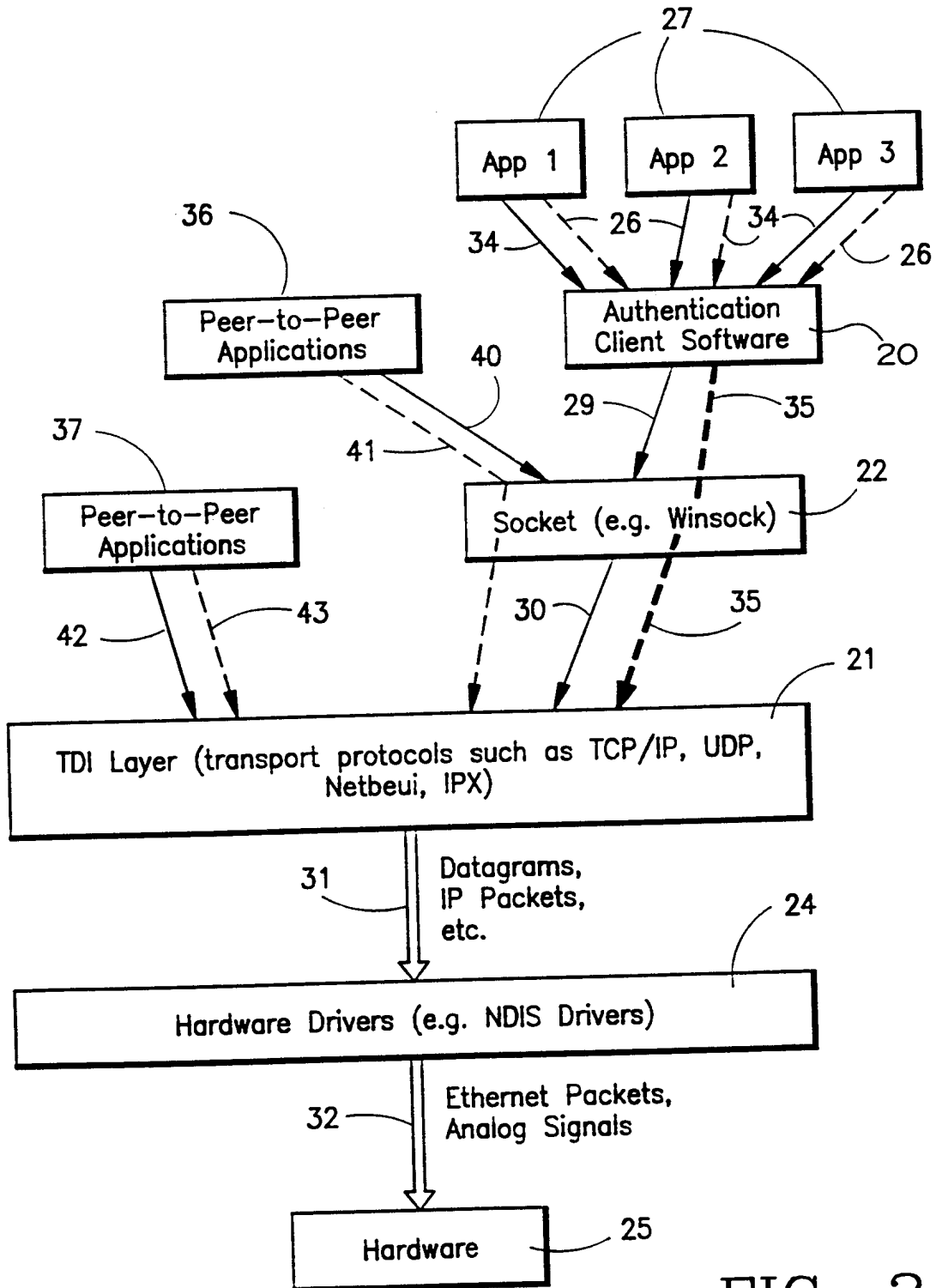


FIG. 2
(PRIOR ART)

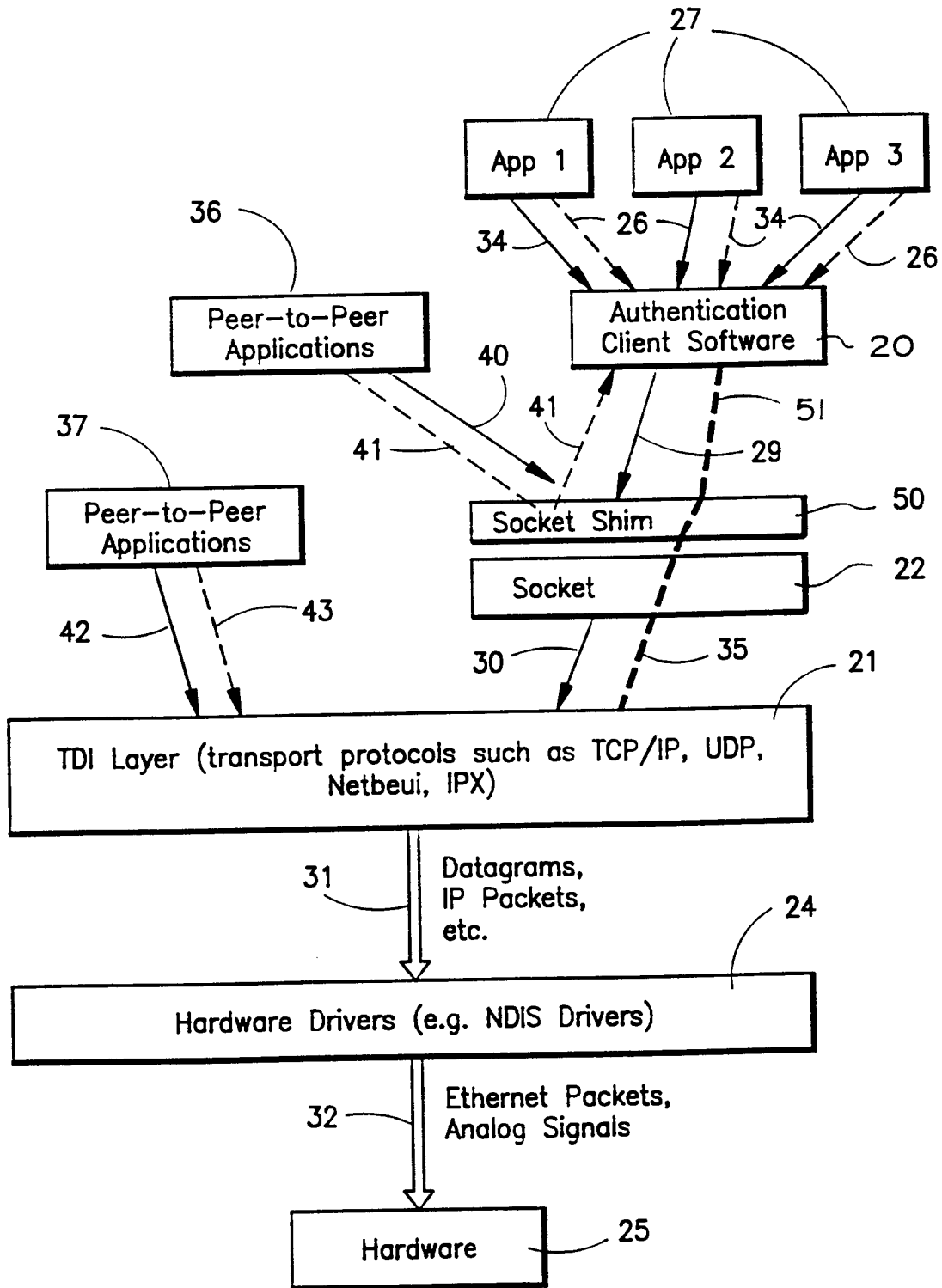


FIG. 3

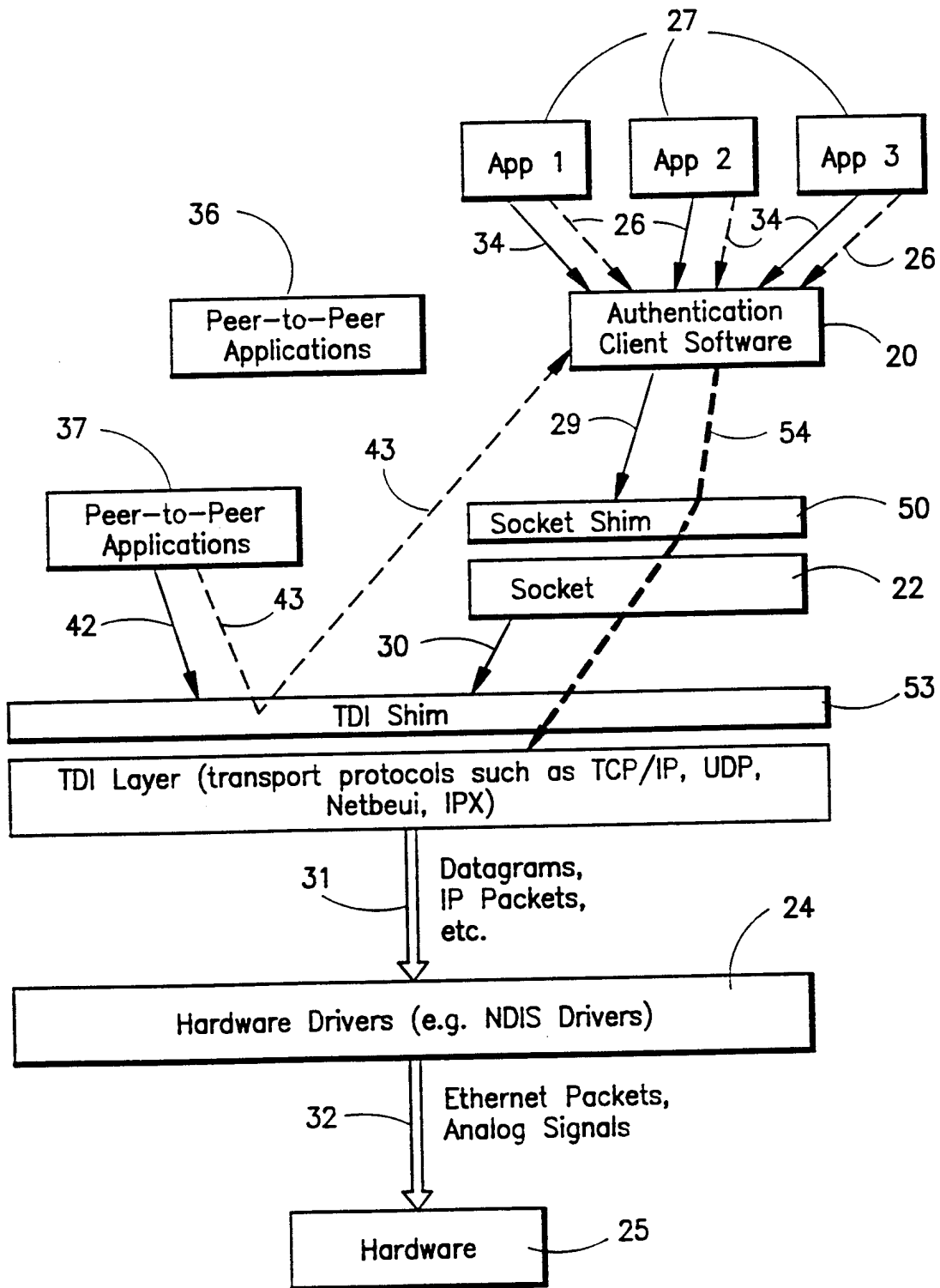


FIG. 4

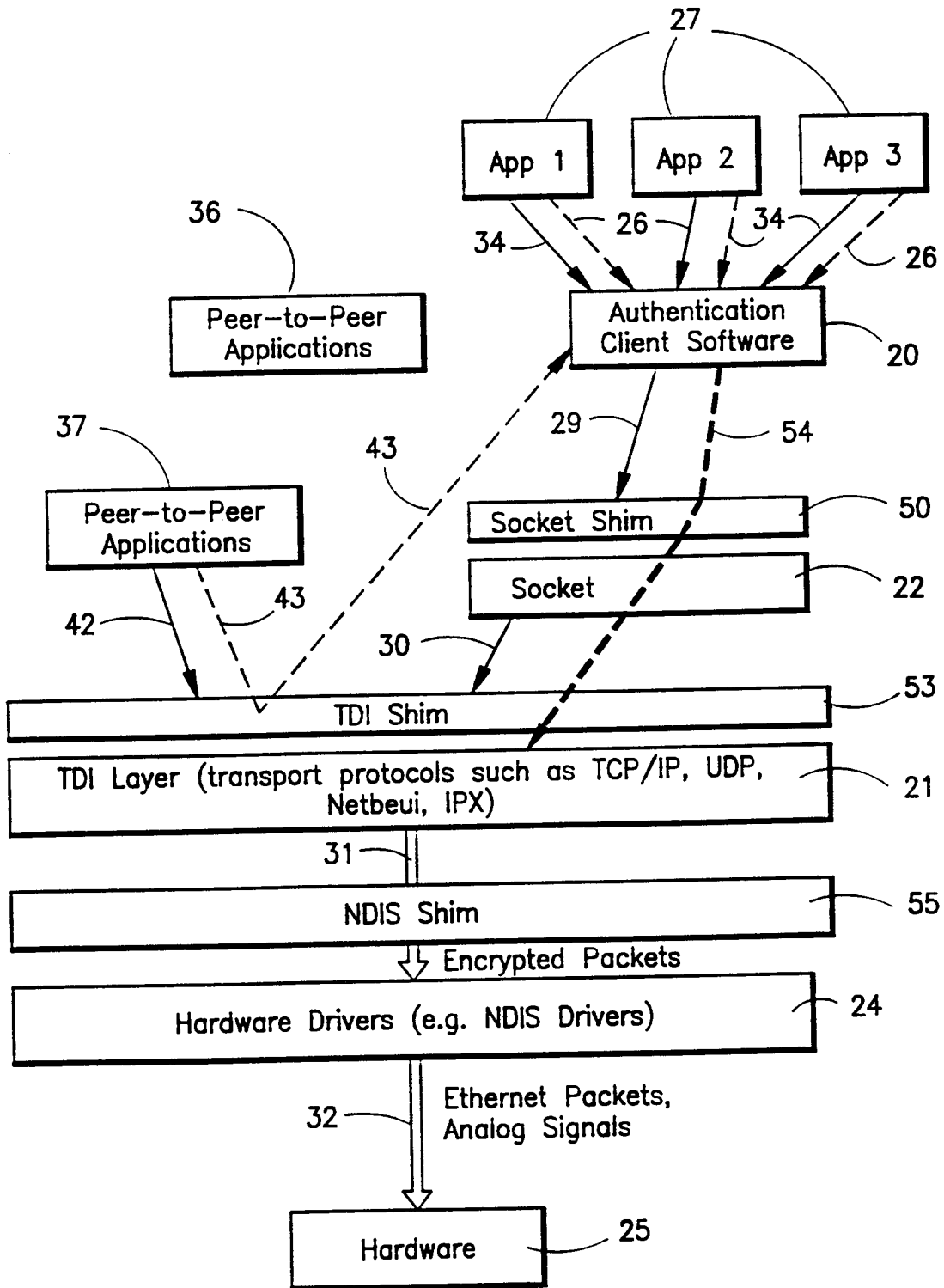


FIG. 5

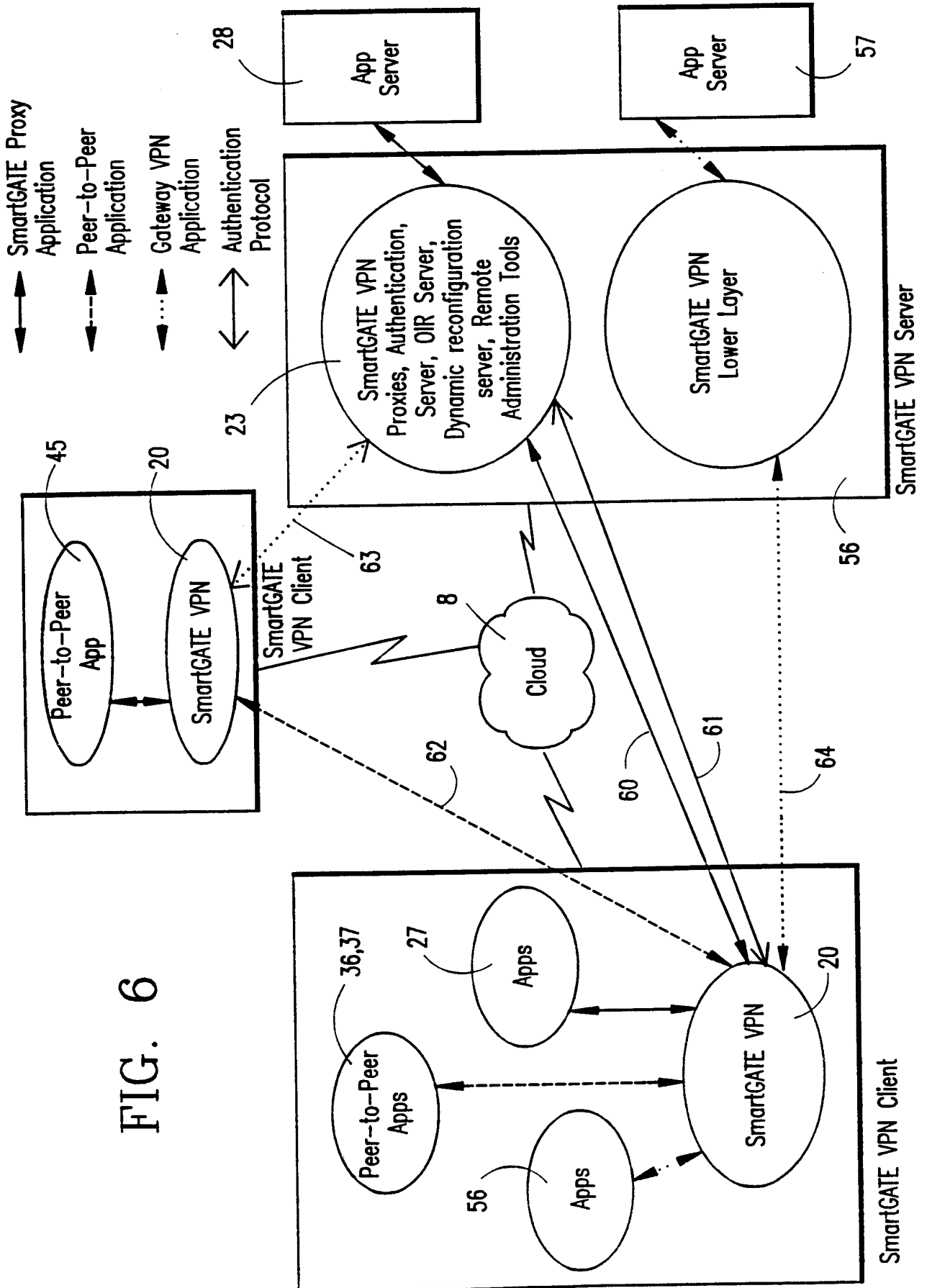


FIG. 6

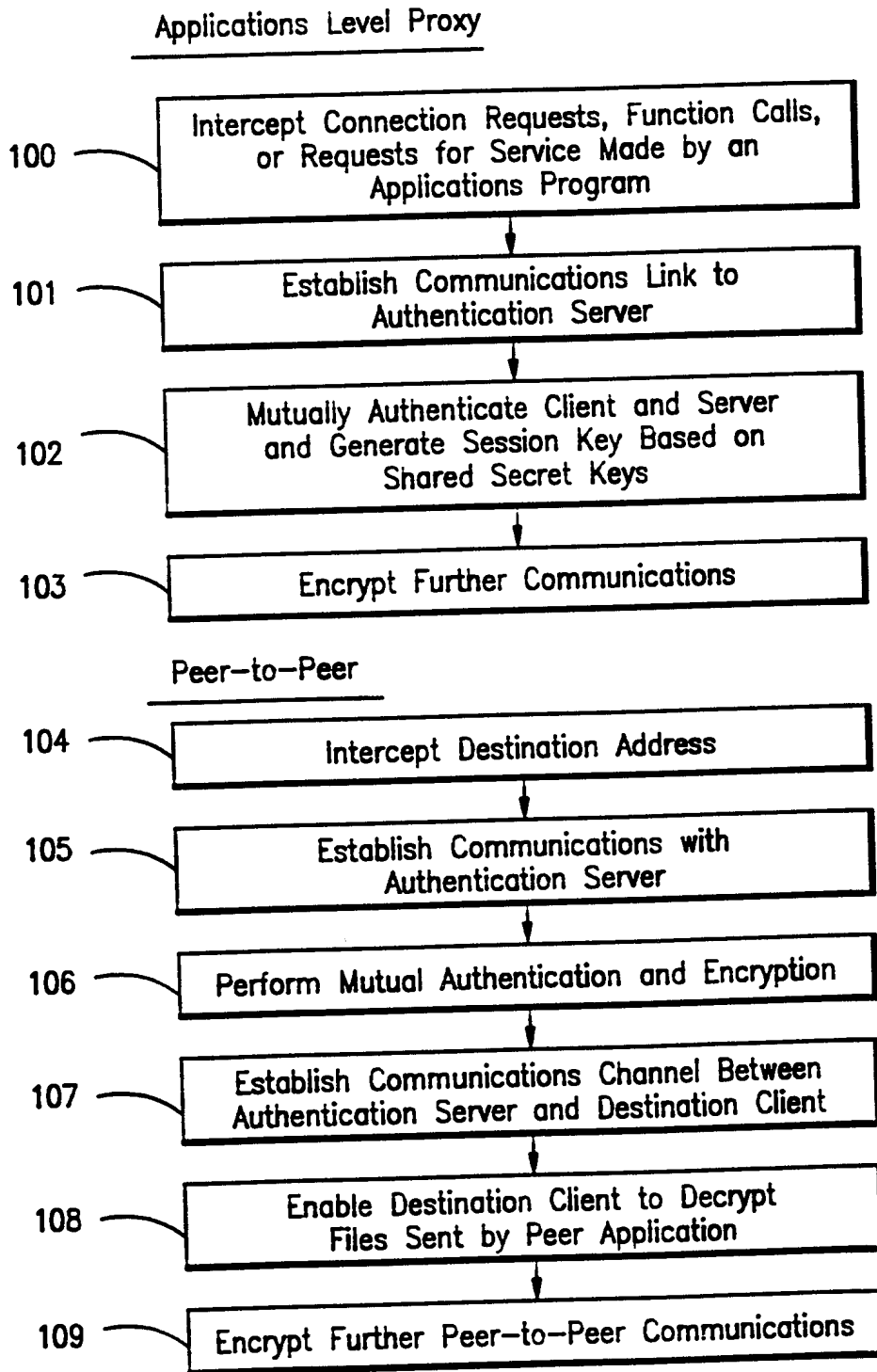


FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/17198

A. CLASSIFICATION OF SUBJECT MATTER IPC(6) :H04L 9/00 US CL :395/187.01 According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) U.S. : 395/187.01, 186, 188.01, 200.17, 200.12; 380/49, 21, 25, 4 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) APS, STN, IEEE ProQuest search terms: virtual private network, shims, DLLs, protocol layers, Winsock, sockets, encryption, authentication.		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,657,390 A (ELGAMAL ET AL) 12 AUGUST 1997, FIGURES 1-8, COL. 3, LINES 20-55, COL. 5, LINE 15 TO COL. 8, LINE 32, COL. 11, LINE 1 TO COL. 16, LINE 49.	1, 5, 6, 16, 17, 18, 19, 23, 31
A	US 5,602,918 A (CHEN ET AL) 11 FEBRUARY 1997, SEE ENTIRE PATENT.	1-34
A	US 5,550,984 A (GELB) 27 AUGUST 1996, ABSTRACT, COL. 3, LINE 52 TO COL. 4, LINE 45, COL.6, LINES 27-55.	1-34
Y	HURWICZ, A VIRTUAL PRIVATE AFFAIR, BYTE MAGAZINE, JULY 1997, PAGES 79-87.	1, 5, 6, 16, 17, 18, 19, 23, 31
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* Special categories of cited documents:	*T*	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
A document defining the general state of the art which is not considered to be of particular relevance	*X*	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
E earlier document published on or after the international filing date	*Y*	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
L document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	*Z*	document member of the same patent family
O document referring to an oral disclosure, use, exhibition or other means		
P document published prior to the international filing date but later than the priority date claimed		
Date of the actual completion of the international search 22 OCTOBER 1998	Date of mailing of the international search report 12 NOV 1998	
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer <i>JOSEPH PALYS</i> Telephone No. (703) 305-9600	

(43) Date of A Publication 11.08.1999

(21) Application No **9802545.5**

(22) Date of Filing **06.02.1998**

(71) Applicant(s)
NEC Technologies (UK) Ltd
(Incorporated in the United Kingdom)
Castle Farm Campus, Priorslee, TELFORD, Shropshire,
TF2 9SA, United Kingdom

(72) Inventor(s)
Charles Marie Herve Noblet

(74) Agent and/or Address for Service
J W White
NEC Technologies (UK) Ltd, Level 3, The Imperium,
Imperial Way, READING, Berks, RG2 0TD,
United Kingdom

(51) INT CL⁶
H04Q 7/32

(52) UK CL (Edition Q)
H4L LDSC

(56) Documents Cited
US 5613204 A **US 5109403 A**

(58) Field of Search
 UK CL (Edition P) **H4L LDSC LDSU LECC LECX**
 INT CL⁶ **H04Q 7/32 7/38**
Online: WPI

(54) Abstract Title
Over-the-air re-programming of radio transceivers

(57) A method of downloading reprogramming data from a network for installation in a mobile station makes use of a dedicated small bandwidth pilot channel. The mobile station obtains from the base station the radio access parameters of a second channel. The second channel is a large bandwidth (bootstrap) channel suitable for fast transfer of data. The bootstrap channel is logically mapped onto a local transmission mode such as DECT or GSM by the mobile station and re-programming data may be downloaded from the base station via the bootstrap channel.

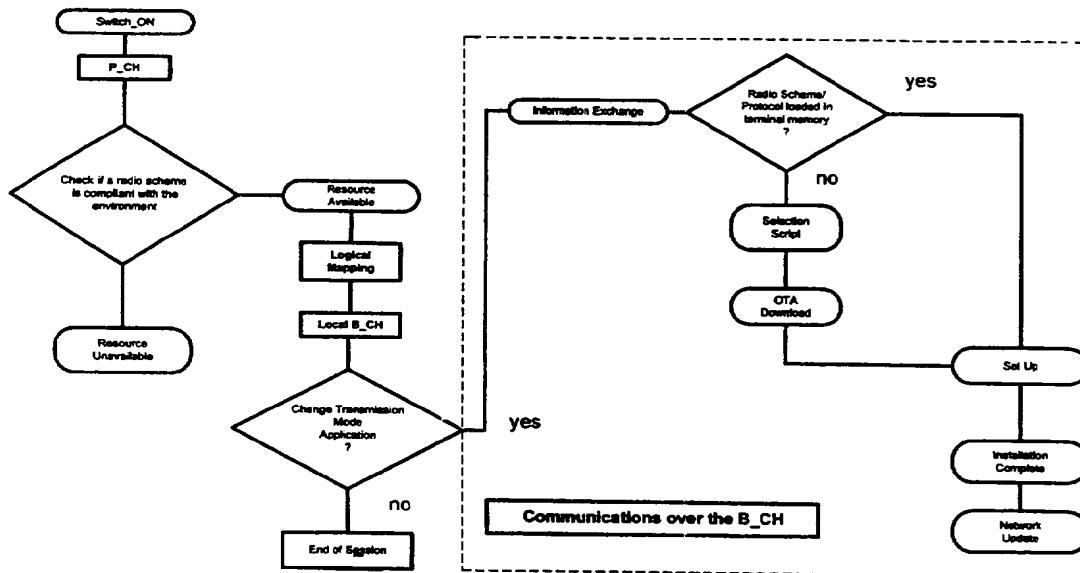


Figure 2

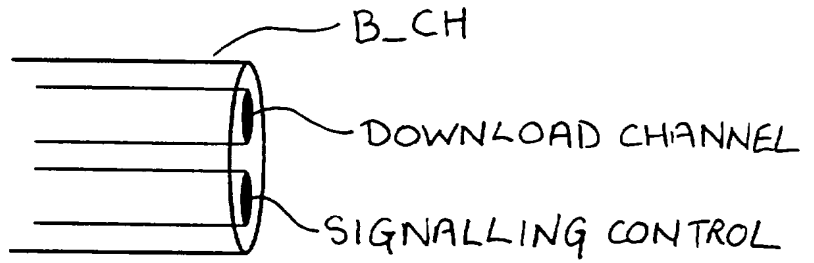


Figure: 1

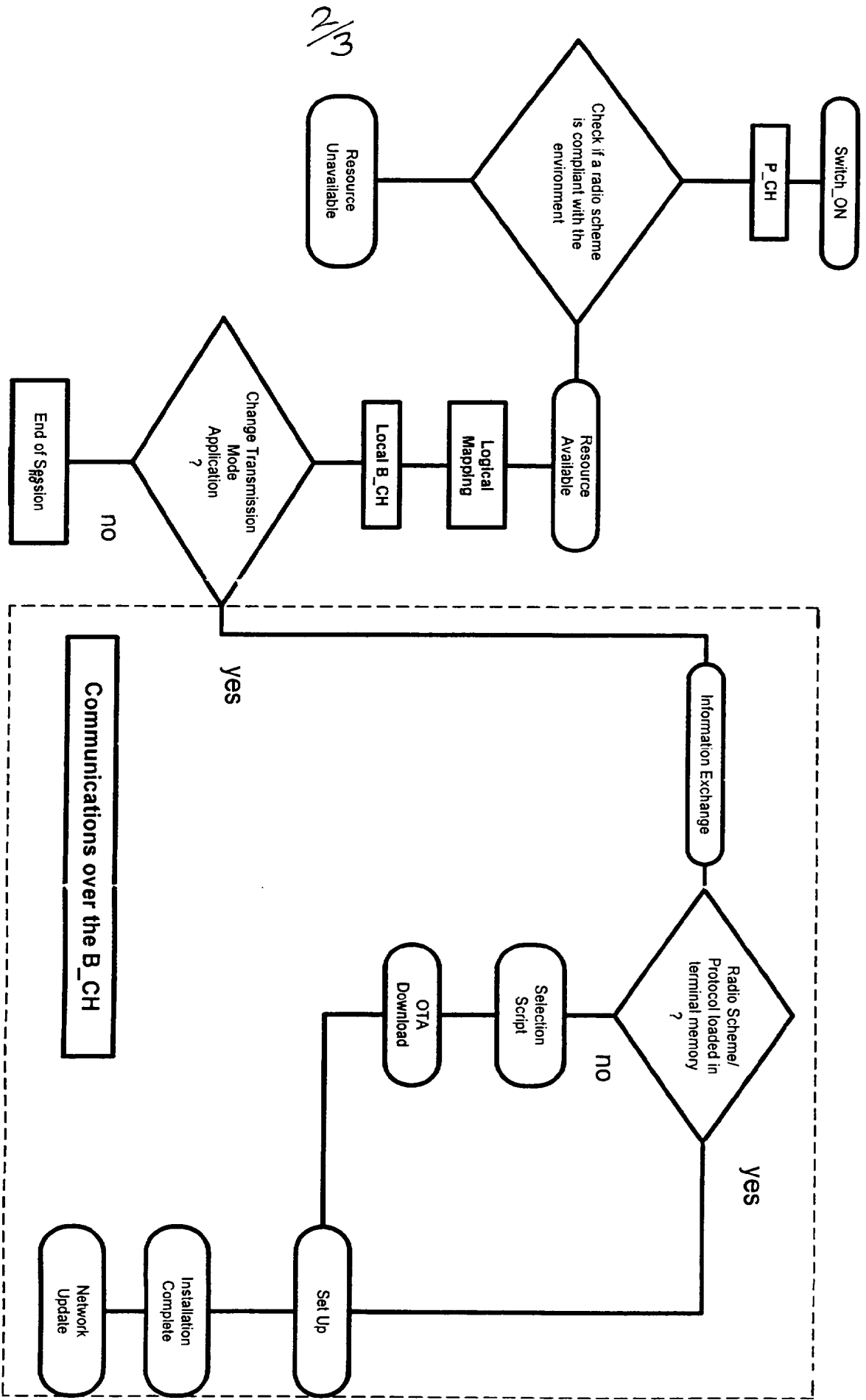


Figure 2

2/3

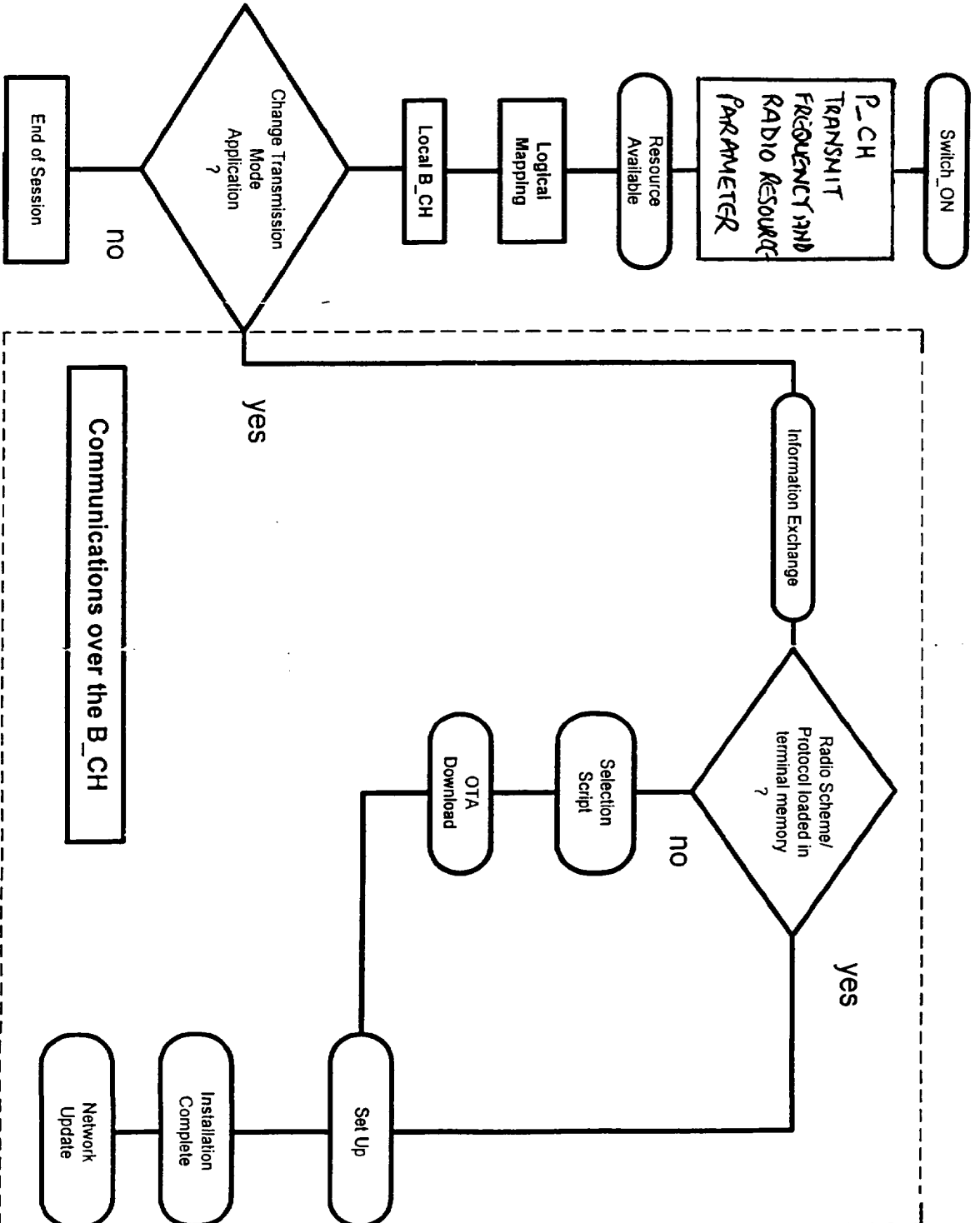


Figure 3

Over-the-air re-programming of radio transceivers

This invention relates to radio transmitter/receivers and in particular it relates to a method of re-programming radio transmitter/receivers over-the-air.

A radio transmitter/receiver (transceiver) such as a radiotelephone is designed for operation with particular types of networks such as GSM 900 or DCS 1800. Intended use of the radiotelephone with a particular network(s) in a restricted geographical area, however, requires that the telephone be configured so as properly to communicate with the particular network (s). The user of a radiotelephone will usually have a telephone which has been configured for communication with a so called "home network". The home network is the local network usually most used by the subscriber.

The area within which a user of e.g. a GSM radiotelephone may operate, however, is considerable and is not limited to the home network but may be used on many other networks throughout the world. Use of a handset outside the home network is known as "roaming".

When the radiotelephone is to be used in roaming it is often necessary for it to have a configuration different to that for use with the home network. It is possible for re-configuration of radio transmitter/receivers to be effected by means of signals received across the air interface.

It is also convenient for the radio to be re-configurable over the air interface so as to support different types of communication and user applications e.g. addition of address book manager, whether or not it is located in the home network.

Over the air re-programming of radio receivers is well known in the art and reference may be made to US patent 5 381 138 for example. The capability to obtain programming data from a network is particularly useful for a roaming radio transmitter/receiver.

When beginning operation in an area for which the radiotelephone is not configured and it is required to download the data for reconfiguration from one of the available networks, a communication link must first be established with the network of interest. It has been proposed that a pilot channel be established in all areas from which the roaming radiotelephone may obtain the data necessary for reconfiguration.

A pilot channel of this type, however, will require a relatively large bandwidth to allow a sufficiently fast transfer of the data required.

According to the invention there is provided a method of downloading reprogramming data from a network for installation in a radio transmitter/receiver comprising initial communication from a first dedicated channel of relatively small bandwidth broadcasting at least the frequency and radio access parameters of a second channel of relatively large bandwidth from which reprogramming data may be downloaded.

Examples of the invention will now be described in more detail with reference to the accompanying figures in which

figure 1 Illustrates the logical structure of the bootstrap channel

figure 2 Is a flow diagram of a reconfiguration process

figure 3 Is a flow diagram of an alternative reconfiguration process

A roaming radio transmitter/receiver (mobile) is located in a region served by one or more networks and the user wishes to communicate with a network from which he can obtain reprogramming data and subsequently begin communicating with the network in the communication mode selected.

A pilot channel broadcast is maintained in the region and contained in the pilot channel broadcast there is at least sufficient information for the mobile to connect to a second channel which we shall call the bootstrap channel. Conveniently the pilot channel will be broadcast in all regions over a standardised radio interface. Only a small bandwidth is required for the pilot channel because of the small amount of information contained in the broadcast.

The small bandwidth requirement makes the task of standardisation much easier with respect to the pilot channel. The wider bandwidth channels are more conveniently assigned locally for ease of implementation.

The Pilot Channel (P_CH) broadcasts a list of sets of parameters corresponding to networks available in the region. The mobile receives the network transmission through the P_CH. If the existing configuration of the mobile is matched to the available regional radio schemes, then a second channel the bootstrap channel (B_CH) is logically mapped onto the selected transmission mode. The base station and mobile exchange information over this dedicated logical channel.

The Bootstrap channel is logically mapped on top of one of the default modes of the terminal; a mapping of a logical B_CH onto the physical GSM channel for instance may be implemented. Once the mapping has been effected the terminal may download data from the base station. The bootstrap channels provided by each operator may accommodate differing services with regard to the applications available for downloading.

The flow diagram shown at fig 3 depicts a reconfiguration procedure.

When the mobile is switched on, it reads the Pilot Channel broadcast. The mobile must be configured to support the (standardised) radio interface of the Pilot Channel. The Pilot Channel carries local radio parameters (standards supported in the regional environment in which the mobile is located). After processing the received information, the mobile

communicates with the base station through the Bootstrap Channel, provided that the mobile has the minimum resources required by its local radio environment. Prior to the change of channel, P_CH to B_CH, a logical mapping of the Bootstrap Channel is performed within the mobile on the selected air interface.

When operation on a local B_CH transmission has been established, the user may wish to change some properties or the performance of his mobile and can request supply of the desired services from the network. If no changes are required then the mobile adopts the default transmission mode in stand-by and releases the allocated B_CH.

If the user requests a change then communication between the base station and mobile is maintained for the exchange, the nature of which will depend on the capabilities of both mobile and network. At least 3 conditions can affect the nature of this information exchange.

Firstly, the mobile may not be able to support the required software. Where the mobile is not able to support the required software, no communication channel is available to the mobile from the existing network resources and use of the mobile within the region will therefore not be possible.

Secondly, the required software may be stored already in the mobile's memory. In this situation there is no need to download a software module but the allocated B_CH connection is maintained for further operations as described.

Thirdly, the software module required to support a different type of communication or user application may need to be downloaded from the base station. Where the download of a software module is required, initially a selection script is downloaded to the mobile followed by downloading and installation of the required software.

When the installation of the required software into the mobile has been completed, the mobile signals to the network the achievement of correct reconfiguration. On receipt of the "correct reconfiguration" signal from the mobile details of the mobile identity and its present configuration are entered on the network database (to license the product for instance) .

With reference to figure 1, the logical structure of the bootstrap channel will include 2 logical sub-channels : a download channel and a signalling control channel (S_CH). The signalling control channel assists in the reduction of errors in transmission so as to allow correct software download.

In the above example, the first channel, the Pilot Channel, is standardised and the mobile must be configured to support the radio interface for the Pilot Channel. The second (bootstrap) channel may be subject to local definition through logical mapping on a local transmission mode e.g. GSM, DECT and the mobile is not initially configured to support the radio interface for the bootstrap channel..

An example of a method of reprogramming providing greater flexibility will now be given. In this example the mobile is configured to support the radio interfaces for both the first, dedicated relatively small bandwidth (Pilot) channel and the second relatively large bandwidth (bootstrap) channel. That is to say that when the mobile is switched on in most and preferably all regions, the network can communicate with the mobile via both pilot and bootstrap channels.

In order for the mobile always to have the appropriate radio interface for the bootstrap channel then this channel would need also to be standardised (in addition to the Pilot Channel). The parameters of the bootstrap channels provided in different regions may have local variations in terms of e.g. allocated frequency, data rate and available user applications.

With reference to figure 3 which is a flow diagram of the reconfiguration process for this example, the mobile when switched on reads the Pilot Channel broadcast. The allocated frequency and radio resource parameters for the bootstrap channel contained in the pilot channel broadcast are processed and any required logical mapping effected. After processing the received information, the mobile communicates with the base station through the Bootstrap Channel.

The condition likely to be experienced in the previous example whereby the mobile is not able to support the required software and no communication channel is available to the mobile from the existing network resources does not apply in this arrangement. The communication via the bootstrap

channel allows the request for and supply of the software module necessary to establish communication with the network. The transfer to the bootstrap channel does not depend on the existing configuration of the mobile since the bootstrap channel is standardised in this example and the mobile is equipped to interface, via the pilot channel, with the bootstrap channel.

The services and structure offered by the Bootstrap Channel are common for both of the above examples, however, the requirements on the terminals and networks differ.

The bootstrap channel will provide the following services by means of over-the-air (OTA) reconfiguration :

capability Exchange - the terminal provides some information to the network on its current configuration and capabilities.

module Selection : at this stage the user specifies the software that his terminal requires to download. This operation could be compared to an installation script.

data download : transfer of the data. In some cases software code will have to be downloaded whilst in other cases the software may already be implemented in the mobile. In the latter case, a set-up mechanism would be sufficient to initiate the reconfiguration.

Once the mobile and the base station are synchronised on the bootstrap channel, information exchange can begin.

Claims

1. A method of downloading reprogramming data from a network for installation in a radio transmitter/receiver comprising initial communication from a first dedicated channel of relatively small bandwidth broadcasting at least the frequency and radio access parameters of a second channel of relatively large bandwidth from which reprogramming data may be downloaded.
2. A method of downloading reprogramming data from a network as in claim 1 where first, dedicated relatively small bandwidth channel has a standard radio interface common to many network locations.
3. A method of downloading reprogramming data from a network as in claim 2 where second relatively large bandwidth channel has a standard radio interface common to many network locations.
4. A method of downloading reprogramming data from a network as in claims 1 to 3 where first, dedicated relatively small bandwidth channel broadcasts a list of sets of parameters corresponding to networks available in the region.
5. A method of downloading reprogramming data from a network as in claim 1 where the radio transmitter/receiver is configured to support the radio interfaces for both the first, dedicated relatively small bandwidth channel and the second relatively large bandwidth channel.



Application No: GB 9802545.5
Claims searched: 1 to 5

Examiner: Glyn Hughes
Date of search: 17 August 1998

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:
UK CI (Ed.P): H4L (LDSC, LDSU, LECC, LECX)
Int CI (Ed.6): H04Q 7/32, 7/38
Other: Online: WPI

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
X	US 5613204 (HABERMAN ET AL) see in particular column 15 lines 48 to 50	1
X	US 5109403 (SUTPHIN) see abstract	1

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

(12) **UK Patent Application** (19) **GB** (11) **2 340 702** (13) **A**

(43) Date of A Publication 23.02.2000

(21) Application No **9912200.4**
 (22) Date of Filing **25.05.1999**
 (30) Priority Data
 (31) **09087823** (32) **29.05.1998** (33) **US**

(71) Applicant(s)
Sun Microsystems Inc
(Incorporated in USA - Delaware)
901 San Antonio Road, MS Palo Alto-521,
California 94303, United States of America

(72) Inventor(s)
Joseph E Provino

(74) Agent and/or Address for Service
D Young & Co
21 New Fetter Lane, LONDON, EC4A 1DA,
United Kingdom

(51) INT CL⁷
H04L 29/06 // H04L 9/00 12/22 12/46

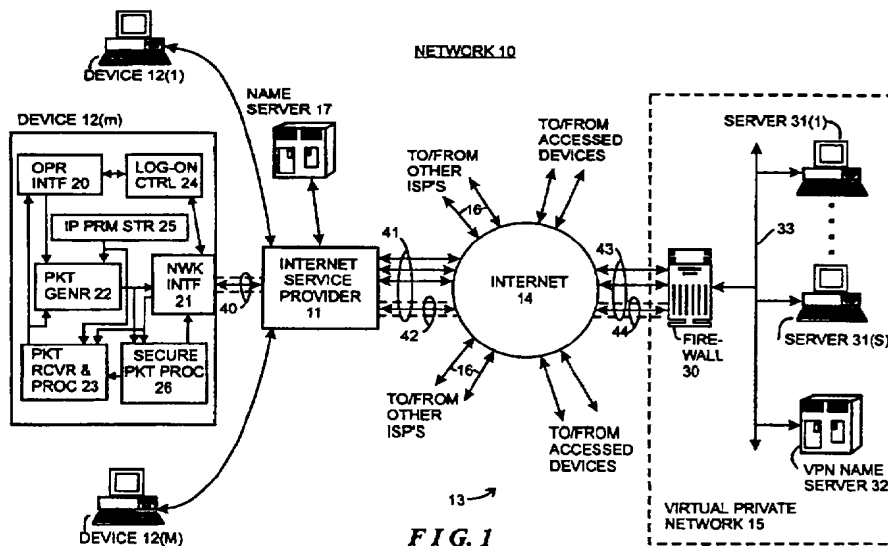
(52) UK CL (Edition R)
H4P PPEB

(56) Documents Cited
EP 0887979 A2 EP 0825748 A2 WO 98/31124 A1

(58) Field of Search
 UK CL (Edition Q) **H4P PPA PPEB PPEC PPG**
 INT CL⁶ **H04L 12/22 12/46 12/66 29/06**
ONLINE DATABASES: WPI, EPODOC, JAPIO

(54) Abstract Title
Accessing a server in a virtual private network protected by a firewall

(57) A virtual private network 15 has a firewall 30, at least one server 31 and a nameserver 32 each having a network address (eg. an n-bit integer address). The server 31 also has a secondary address (eg. a human readable address) and the nameserver 32 provides an association between the secondary address and the network address. An authorised external device 12 establishes a secure tunnel between itself and the firewall for communication using encryption. When the external device requests connection to server 31 using the secondary address of server 31, the firewall provides external device 12 with the network address of the nameserver 32. The external device 12 transmits a request for resolution of the network address associated with the secondary address to the nameserver through the firewall. The nameserver then transmits the network address of the server 31 through the firewall to the external device using the secure tunnel. The external device can thereafter use the network address of server 31 in subsequent communications.



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 2 340 702 A

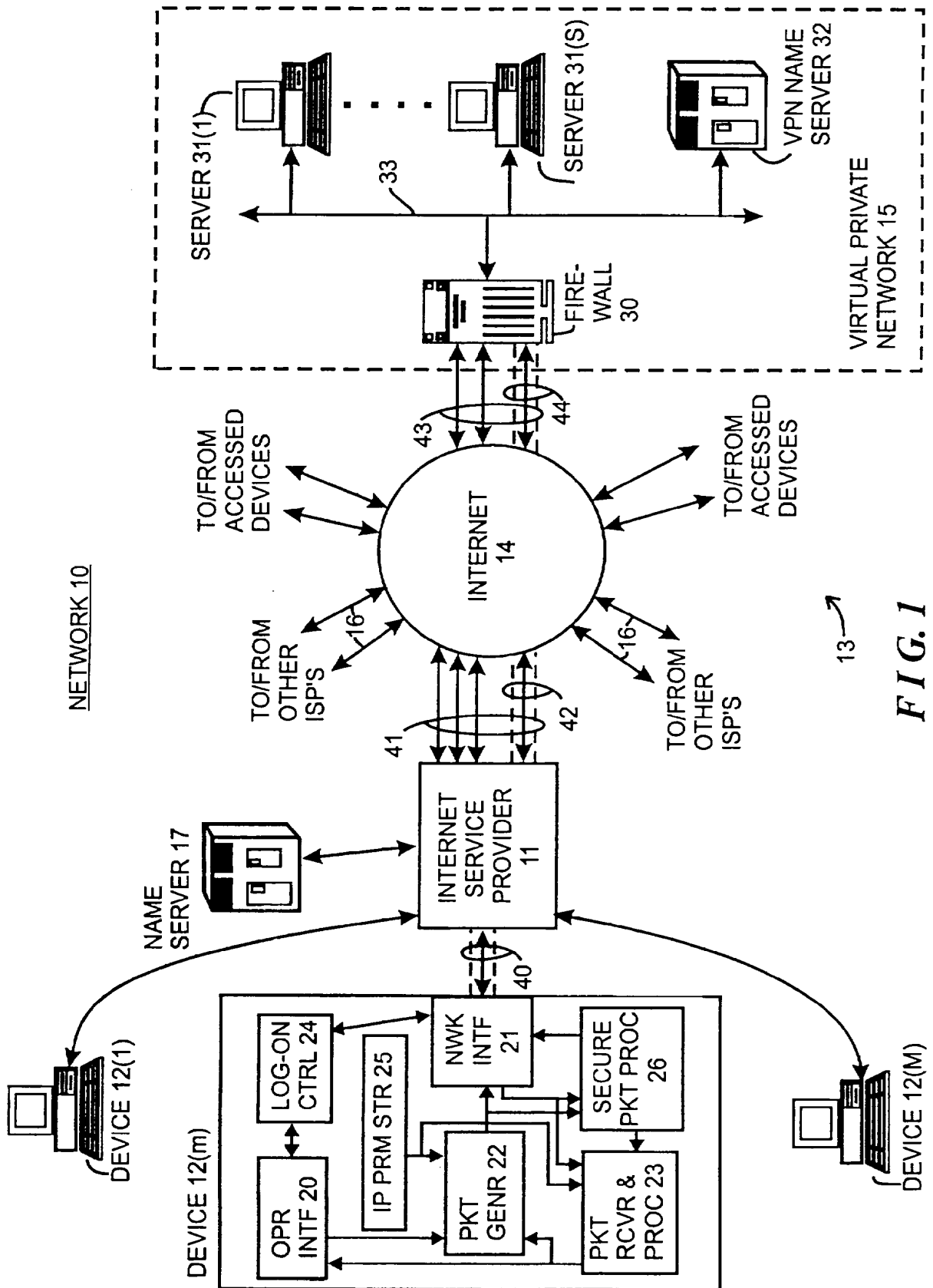


FIG. 1

FIELD OF THE INVENTION

The invention relates generally to the field of digital communications systems and methods, and more particularly to systems and methods for easing communications between devices connected to public networks such as the Internet and devices connected to private networks.

BACKGROUND OF THE INVENTION

Digital networks have been developed to facilitate the transfer of information, including data and programs, among digital computer systems and other digital devices. A variety of types of networks have been developed and implemented, including so-called "wide-area networks" (WAN's) and "local area networks" (LAN's), which transfer information using diverse information transfer methodologies. Generally, LAN's are implemented over relatively small geographical areas, such as within an individual office facility or the like, for transferring information within a particular office, company or similar type of organization. On the other hand, WAN's are generally implemented over relatively large geographical areas, and may be used to transfer information between LAN's as well as between devices that are not connected to LAN's. WAN's also include public networks, such as the Internet, which can carry information for a number of companies.

Several problems have arisen in connection with communication over a network, particularly a large public WAN such as the Internet. Generally, information is transferred over a network in message packets, which are transferred from one device, as a source device, to another device as a destination device, through one or more routers or switching nodes (generally, switching nodes) in the network. Each message packet includes a destination address which the switching nodes use to route the respective message packet to the appropriate destination device. Addresses over the Internet are in the form of an "n"-bit integer (where "n" may be thirty two or 128), which are difficult for a person to remember and enter when he or she wishes to enable a message packet to be transmitted. To relieve a user of the necessity of remembering and entering specific integer Internet

addresses, the Internet provides second addressing mechanism which is more easily utilized by human operators of the respective devices. In that addressing mechanism, Internet domains, such as LAN's, Internet service providers ("ISP's") and the like which are connected in the Internet, are identified by relatively human-readable names. To accommodate the use of human-readable names, nameservers, also referred to as DNS servers, are provided to resolve the human-readable names to the appropriate Internet addresses. When an operator at one device, wishing to transmit a message packet to another device, enters the other device's human-readable name, the device will initially contact a nameserver. Generally, the nameserver may be part of the ISP itself or it may be a particular device which is accessible through the ISP over the Internet; in any case, the ISP will identify the nameserver to be used to the device when the device logs in to the ISP. If, after being contacted by the device, the nameserver has or can obtain an integer Internet address for the human-readable domain name, it (that is, the nameserver) will provide the integer Internet address corresponding to the human-readable domain name to the operator's device. The device, in turn, can thereafter include the integer Internet address returned by the nameserver in the message packet and provide the message packet to the ISP for transmission over the Internet in a conventional manner. The Internet switching nodes use the integer Internet address to route the message packet to the intended destination device.

Other problems arise, in particular, in connection with the transfer of information over a public WAN such as the Internet. One problem is to ensure that information transferred over the WAN that the source device and the destination device wish to maintain confidential, in fact, remains confidential as against possible eavesdroppers which may intercept the information. To maintain confidentiality, various forms of encryption have been developed and are used to encrypt the information prior to transfer by the source device, and to decrypt the information after it has been received by the destination device. If it is desired that, for example, all information transferred between a particular source device and a particular destination device is maintained confidential, the devices can establish a "secure tunnel" therebetween, which essentially ensures that all information to be transferred by the source device to the destination device is encrypted (except for certain

protocol information, such as address information, which controls the flow of network packets through the network between the source and destination devices) prior to transfer, and that the encrypted information will be decrypted prior to utilization by the destination device. The source and destination devices may themselves perform the encryption and decryption, respectively, or the encryption and decryption may be performed by other devices prior to the message packets being transferred over the Internet.

A further problem that arises in particular in connection with companies, government agencies, and private organizations whose private networks, which may be LAN's, WAN's or any combination thereof, are connected to public WAN's such as the Internet, is to ensure that their private networks are secure against others whom the companies do not wish to have access thereto, or to regulate and control access by others whom the respective organizations may wish to have limited access. To accommodate that, the organizations typically connect their private networks to the public WAN's through a limited number of gateways sometimes referred to as "firewalls," through which all network traffic between the internal and public networks pass. Typically, network addresses of domains and devices in the private network "behind" the firewall are known to nameservers which are provided in the private network, but are not available to nameservers or other devices outside of the private network, making communication between a device outside of the private network and a device inside of the private network difficult.

SUMMARY OF THE INVENTION

Particular and preferred aspects of the invention are set out in the accompanying independent and dependent claims. Features of the dependent claims may be combined with those of the independent claims as appropriate and in combinations other than those explicitly set out in the claims.

The invention provides a new and improved system and method for easing communications between devices connected to public networks such as the Internet and devices connected to private networks by facilitating resolution of secondary addresses, such as the Internet's human-readable addresses, to network addresses by nameservers or the like connected to the private networks.

In brief summary, an embodiment of the invention provides a system comprising a virtual private network and an external device interconnected by a digital network. The virtual private network has a firewall, at least one internal device and a nameserver each having a network address. The internal device also has a secondary address, and the nameserver is configured to provide an association between the secondary address and the network address. The firewall, in response to a request from the external device to establish a connection therebetween, provides the external device with the network address of the nameserver. The external device, in response to a request from an operator or the like, including the internal device's secondary address, requesting access to the internal device, generates a network address request message for transmission over the connection to the firewall requesting resolution of the network address associated with the secondary address. The firewall provides the address resolution request to the nameserver, and the nameserver provides the network address associated with the secondary address to the firewall. The firewall, in turn, provides the network address in a network address response message for transmission over the connection to the external device. The external device can thereafter use the network address so provided in subsequent communications with the firewall intended for the internal device.

BRIEF DESCRIPTION OF THE DRAWINGS

Exemplary embodiments of the invention are described hereinafter, by way of example only, with reference to the accompanying drawings, in which:

FIG. 1 is a functional block diagram of a network constructed in accordance with the invention.

DETAILED DESCRIPTION OF AN ILLUSTRATIVE EMBODIMENT

FIG. 1 is a functional block diagram of a network 10 constructed in accordance with the invention. The network 10 as depicted in FIG. 1 includes an Internet service provider ("ISP") 11 which facilitates the transfer of message packets among one or more devices 12(1) through 12(M) (generally identified by reference numeral 12(m)) connected to ISP 11, and other devices, generally identified by reference numeral 13, over the Internet 14, thereby to facilitate the transfer of information in message packets among the devices 12(m) and 13. The ISP 11 connects to the Internet 14 over one or more logical connections or gateways or the like (generally referred to herein as "connections") generally identified by reference numeral 41. The ISP 11 may be a public ISP, in which case it connects to devices 12(m) which may be controlled by operators who are members of the general public to provide access by those operators to the Internet. Alternatively, ISP 11 may be a private ISP, in which case the devices 12(m) connected thereto are generally operated by, for example, employees of a particular company or governmental agency, members of a private organization or the like, to provide access by those employees or members to the Internet.

As is conventional, the Internet comprises a mesh of switching nodes (not separately shown) which interconnect ISP's 11 and devices 13 to facilitate the transfer of message packets thereamong. The message packets transferred over the Internet 14 conform to that defined by the so-called Internet protocol "IP" and include a header portion, a data portion, and may include a error detection and/or correction portion. The header portion includes information used to transfer the message packet through the Internet 14, including, for example, a destination address that identifies the device that is to receive the message packet as the destination device and a source address that identifies the device which generated the message packet. For each message packet, the destination and source addresses are each in the form of an integer that uniquely identifies the respective destination and source devices. The switching nodes comprising the Internet 14 use at least the destination address of each respective message packet to route it (that is, the respective message packet) to the destination device, if the destination device is connected to the Internet, or to an ISP 11 or other device connected to the Internet 14, which, in turn, will forward the message packet to the appropriate destination. The data portion of each message packet includes the data to be transferred

in the message packet, and the error detection and/or correction portion contains error detection and/or correction information which may be used to verify that the message packet was correctly transferred from the source to the destination device (in the case of error detection information), and correct selected types of errors if the message packet was not correctly transferred (in the case of error correction information).

The devices 12(m) connected to ISP 11 may comprise any of a number of types of devices which communicate over the Internet 14, including, for example, personal computers, computer workstations, and the like, with other devices 13. Each device 12(m) communicates with the ISP 11 to transfer message packets thereto for transfer over the Internet 14, or to receive message packets therefrom received by the ISP 11 over the Internet 14, using any convenient protocol such as the well-known point-to-point protocol ("PPP") if the device 12(m) is connected to the ISP 11 using a point-to-point link, any conventional multi-drop network protocol if the device 12(m) is connected to the ISP 11 over a multi-drop network such as the Ethernet, or the like. The devices 12(m) are generally constructed according to the conventional stored-program computer architecture, including, for example, a system unit, a video display unit and operator input devices such as a keyboard and mouse. A system unit generally includes processing, memory, mass storage devices such as disk and/or tape storage elements and other elements (not separately shown), including network and/or telephony interface devices for interfacing the respective device to the ISP 11. The processing devices process programs, including application programs, under control of an operating system, to generate processed data. The video display unit permits the device to display processed data and processing status to the user, and the operator input device enables the user to input data and control processing.

These elements of device 12(m), along with suitable programming, cooperate to provide device 12(m) with a number of functional elements including, for example, an operator interface 20, a network interface 21, a message packet generator 22, a message packet receiver and processor 23, an ISP log-on control 24, an Internet parameter store 25 and, in connection with the invention, a secure message packet processor 26. The operator interface 20 facilitates reception by the device

12(m) of input information from the operator input device(s) of device 12(m) and the display of output information to the operator on the video display device(s) of the device 12(m). The network interface 21 facilitates connection of the device 12(m) to the ISP 11 using the appropriate PPP or network protocol, to transmit message packets to the ISP 11 and receive message packets therefrom. The network interface 21 may facilitate connection to the ISP 11 over the public telephone network to allow for dial-up networking of the device 12(m) over the public telephone system. Alternatively or in addition, the network interface 21 may facilitate connection through the ISP 11 over, for example, a conventional LAN such as the Ethernet. The ISP log on control 24, in response to input provided by the operator interface 20 and/or in response to requests from programs (not shown) being processed by the device 12(m), communicates through the network interface 21 to facilitate the initialization ("log-on") of a communications session between the device 12(m) and the ISP 11, during which communications session the device 12(m) will be able to transfer information, in the form of, message packets with other devices over the Internet 14, as well as other devices 12(m') (m'≠m) connected to the ISP 11 or to other ISP's. During a log-on operation, the ISP log-on control 24 receives the Internet protocol ("IP") parameters which will be used in connection with message packet generation during the communications session.

During a communications session, the message packet generator 22, in response to input provided by the operator through the operator interface 20, and/or in response to requests from programs (not separately shown) being processed by the device 12(m), generates message packets for transmission through the network interface 21. The network interface 21 also receives message packets from the ISP 11 and provides them to message packet receiver and processor 23 for processing and provision to the operator interface 20 and/or other programs (not shown) being processed by the device 12(m). If the received message packets contain information, such as Web pages or the like, which is to be displayed to the operator, the information can be provided to the operator interface 20 to enable the information to be displayed on the device's video display unit. In addition or alternatively, the information may be provided to other programs (not shown) being processed by the device 12(m) for processing.

Generally, elements such as the operator interface 20, message packet generator 22, message packet receiver and processor 23, ISP log-on control 24 and Internet parameter store 25 may comprise elements of a conventional Internet browser, such as Mosaic, Netscape Navigator and Microsoft Internet Explorer.

In connection with the invention, as noted above the device 12(m) also includes a secure message packet processor 26. The secure message packet processor 26 facilitates the establishment and use of a "secure tunnel," which will be described below, between the device 12(m) and another device 12 (m') (m'≠m) or 13. Generally, in a secure tunnel, information in at least the data portion of message packets transferred between device 12(m) and a specific other device 12(m') (m'≠m) or 13 is maintained in secret by, for example, encrypting the data portion prior to transmission by the source device. Information in other portions of such message packets may also be maintained in secret, except for the information that is required to facilitate the transfer of the respective message packet between the devices, including, for example, at least the destination information, so as to allow the Internet's switching nodes and ISP's to identify the device that is to receive the message packet.

In addition to ISP 11, a number of other ISP's may connect to the Internet, as represented by arrows 16, facilitating communications between devices which are connected to those other ISP's with other devices over the Internet, which may include the devices 12(n) connected to ISP 11.

The devices 13 which devices 12(m) access and communicate with may also be any of a number of types of devices, including personal computers, computer workstations, and the like, and also including mini-and mainframe computers, mass storage systems, compute servers, local area networks ("LAN's") and wide area networks ("WAN's") including such devices and numerous other types of devices which may be connected directly or indirectly to the networks. In connection with the invention, at least one of the devices will include at least one private network, identified as virtual private network 15, which may be in the form of a LAN or WAN. The virtual private network 15 may comprise any of the devices 12(m') (m'≠m) (thereby connecting to the Internet 14

through an ISP) or 13 (thereby connecting directly to the Internet 14); in the illustrative embodiment described herein, the virtual private network 15 will be assumed to comprise a device 13. The virtual private network 15 itself includes a plurality of devices, identified herein as a firewall 30, a plurality of servers 31(1) through 31(S) (generally identified by reference numeral 31(s)) and a nameserver 32, all interconnected by a communication link 33. The firewall 30 and servers 31(s) may be similar to any of the various types of devices 12(m) and 13 described herein, and thus may include, for example, personal computers, computer workstations, and the like, and also including mini-and mainframe computers, mass storage systems, compute servers, local area networks ("LAN's") and wide area networks ("WAN's") including such devices and numerous other types of devices which may be connected directly or indirectly to the networks.

As noted above, the devices, including devices 12(m) and devices 13, communicate by transferring message packets over the Internet. The devices 12(m) and 13 can transfer information in a "peer-to-peer" manner, in a "client-server" manner, or both. Generally, in a "peer-to-peer" message packet transfer, a device merely transfers information in one or more message packets to another device. On the other hand, in a "client-server" manner, a device, operating as a client, can transfer a message packet to another device, operating as a server to for example, initiate service by the other device. A number of types of such services will be appreciated by those skilled in the art, including, for example, the retrieval of information from the other device, to enable the other device to perform processing operations, and the like. If the server is to provide information to the client, it (that is, the server) may generally be referred to as a storage server. On the other hand, if the server is to perform processing operations at the request of the client, it (that is, the server) may generally be referred to as a compute server. Other types of servers, for performing other types of services and operations at the request of clients, will be appreciated by those skilled in the art.

In a client/server arrangement, device 12(m) requiring service by, for example, a device 13, generates one or more request message packets requesting the required service, for transfer to the device 13. The request message packet includes the Internet address of the device 13 that is, as the destination device, to receive the message packet and perform the service. The device 12(m)

transfers the request message packet(s) to the ISP 11. The ISP 11, in turn, will transfer the message packet over the Internet to the device 13. If the device 13 is in the form of a WAN or LAN, the WAN or LAN will receive the message packet(s) and direct it (them) to a specific device connected therein which is to provide the requested service.

In any case, after the device 13 which is to provide the requested service receives the request message packet (s), it will process the request. If the device 12(m) which generated the request message packet(s), or its operator, has the required permissions to request the service from the device 13 which generated the request message packet, if the requested service is to initiate the transfer of information from the device 13 as a storage server to the device 12(m) as client, the device 13 will generate one or more response message packets including the requested information, and transmit the packet(s) over the Internet 14 to the ISP 11. The ISP 11, in turn, will transfer the message packet(s) to the device 12(m). On the other hand, if the requested service is to initiate processing by the device 13 as a compute server, the device 13 will perform the requested computation service(s). In addition, if the device 13 is to return processed data generated during the computations to the device 12(m) as client, the device 13 will generate one or more response message packet(s) including the processed data and transmit the packet(s) over the Internet 14 to the ISP 11. The ISP 11, in turn, will transfer the message packet(s) to the device 12(m). Corresponding operations may be performed by the devices 12(m) and 13, ISP 11 and Internet 14 in connection with other types of services which may be provided by the server devices 13.

As noted above, each message packet that is generated by devices 12(m) and 13 for transmission over the Internet 14 includes a destination address, which the switching nodes use to route the respective message packet to the appropriate destination device. Addresses over the Internet are in the form of an "n"-bit integer (where "n" currently may be thirty two or 128). To relieve, in particular, an operator of a device 12(m) of the necessity of remembering specific integer Internet addresses and providing them to the device 12(m) to initiate generation of a message packet for transmission over the Internet, the Internet provides a second addressing mechanism which is more easily utilized by human operators of the respective devices. In that addressing mechanism,

Internet domains, such as LAN's, Internet service providers ("ISP's") and the like which are connected in the Internet, are identified by relatively human-readable names. To accommodate human-readable domain names, ISP 11 is associated with a nameserver 17 (which may also be referred to as a DNS servers), which can resolve the human-readable domain names to provide the appropriate Internet address for the destination referred to in the respective human-readable name. Generally, the nameserver may be part of or connected directly to the ISP 11, as shown in FIG. 1, or it may be a particular device which is accessible through the ISP over the Internet. In any case, as noted above, when the device 12(m) logs on to the ISP 11 during a communications session, the ISP 11 will assign various Internet protocol ("IP") parameters which the device 12(m) is to use during the communications session, which will be stored in the Internet parameter store 25. These IP parameters include such information as

(a) an Internet address for the device 12(m) which will identify the device 12(m) during the communications session, and

(b) the identification of a nameserver 17 that the device 12(m) is to use during the communications session.

The device 12(m), when it generates message packets for transfer, will include its Internet address (item (a) above) as the source address. The device(s)13 which receives the respective message packets can use the source address from message packets received from the device 12(m) in message packets which they (that is, device(s) 13) generate for transmission to the device 12(m), thereby to enable the Internet to route the message packets generated by the respective device 13 to the device 12(m). If the device 12(m) is to access the nameserver 17 over the Internet 14, the nameserver identification provided by the ISP 11 (item (b) above) will be in the form of an integer Internet address which will allow the device 12(m) to generate messages to the nameserver 17 requesting resolution of human-readable Internet addresses into integer Internet addresses. The ISP 11 may also assign other IP parameters to the device 12(m) when it logs on to the ISP 11, including, for example, the identification of a connection to the Internet 14 that is to be used for messages transmitted by the

device 12(m), particularly if the ISP 11 has multiple gateways. Generally, the device 12(m) will store the Internet parameters in the Internet parameter store 25 for use during the communications session.

When an operator operating device 12(m) wishes to enable the device 12(m) to transmit a message packet to a device 13, he or she provides the Internet address for the device 13 to the device 12(m), through the operator interface 20, and information, or the identification of information maintained by the device 12(m) that is to be transmitted in the message. The operator interface 20, in turn, will enable the packet generator 22 to the required packets for transmission through the ISP 11 over the Internet 11. If

(i) the operator has provided the integer Internet address, or

(ii) the operator has provided the human-readable Internet address, but the packet generator 22 already has the integer Internet address which corresponds to the human-readable Internet address provided by the operator,

the packet generator 22 may generate the packets directly upon being enabled by the operator interface 20, and provide them to the network interface 21 for transmission to the ISP 11.

However, if the operator has provided the human-readable Internet address for the device 13 to which the packets are to be transferred, and if the packet generator 22 does not already have the corresponding integer Internet address therefor, the packet generator 22 will enable the network address to be obtained from the nameserver 17 identified in the IP parameter store 25. In that operation, the packet generator 22 will initially contact nameserver 17 to attempt to obtain the appropriate integer Internet address from the nameserver 17. In these operations, the device 12(m) will generate appropriate message packets for transmission to the nameserver 17, using the nameserver's integer Internet address as provided by the ISP 11 when it (that is, the device 12(m)) logs on at the beginning of the communications session. In any case, if the nameserver 17 has or can obtain the integer Internet address for the human-readable name, it (that is, the nameserver 17) will

provide the integer Internet address to the device 12(m). The integer Internet address will be received by the packet generator 22 through the network interface 21 and packet receiver and processor 23. After the packet generator 22 receives the integer Internet address, it can generate the necessary message packets for transmission to the device 13 through the network interface 21 and ISP 11.

As noted above, one of the devices 13 connected to the Internet 14 is virtual private network 15, the virtual private network 15 including a firewall 30, a plurality of devices identified as servers 31(s), and a nameserver 32 interconnected by a communication link 33. The servers 31(s), firewall 30 and nameserver 32 can, as devices connected in a LAN or WAN, transfer information in the form of message packets thereamong. Since the firewall 30 is connected to the Internet 14 and can receive message packets thereover it has an Internet address. In addition, at least the servers 31(s) which can be accessed over the Internet also have respective Internet addresses, and in that connection the nameserver 32 serves to resolve human-readable Internet addresses for servers 31(s) internal to the virtual private network 15 to respective integer Internet addresses.

Generally, the virtual private network 15 is maintained by a company, governmental agency, organization or the like, which desires to allow the servers 31(s) to access other devices outside of the virtual private network 15 and transfer information thereto over the Internet 14, but which also desires to limit access to the servers 31(s) by devices 12(m) and other devices over the Internet 14 in a controlled manner. The firewall 30 serves to control access by devices external to the virtual private network 15 to servers 31(s) within the virtual private network 15. In that operation, the firewall 30 also connects to the Internet 14, receives message packets therefrom for transfer to a server 31(s). If the message packet indicates that the source of the message packet is requesting access to the particular server 31(s), and if the source is authorized to access the server 31(s), the firewall 30 will forward the message packet over the communication link 33 to the server 31(s). On the other hand if the source is not authorized to access the server 31(s), the firewall 30 will not forward the message packet to the server 31(s), and may, instead, transmit a response message packet to the source device indicating that the source was not authorized to access the server 31(s). The

firewall may be similar to other devices 31(s) in the virtual private network 15, with the addition of one or more connections to the Internet, which are generally identified by reference numeral 43.

Communications between devices external to the virtual private network 15, such as device 12(m), and a device, such as a server 31(s), inside the virtual private network 15, may be maintained over a secure tunnel between the firewall 30 and the external device as described above to maintain the information transferred therebetween secret while being transferred over the Internet 14 and through the ISP 11. A secure tunnel between device 12(m) and virtual private network 15 is represented in FIG. 1 by logical connections identified by reference numerals 40, 42, and 44; it will be appreciated that the logical connection 42 comprises one of the logical connections 41 between ISP 11 and Internet 14, and logical connection 44 comprises one of the logical connections 43 between the Internet 14 and the firewall 30.

Establishment of a secure tunnel can be initiated by device 12(m) external to the virtual private network 15. In that operation, the device 12(m), in response to a request from its operator, generates a message packet for transfer through the ISP 11 and Internet 14 to the firewall 30 requesting establishment of a secure tunnel between the device 12(m) and firewall 30. The message packet may be directed to a predetermined integer Internet address associated with the firewall 30 which is reserved for secure tunnel establishment requests, and which is known to and provided to the device 12(m) by the nameserver 17. If the device 12(m) is authorized to access a server 31(s) in the virtual private network 15, the client 12(m) and firewall 30 engage in a dialog, comprising one or more message packets transferred therebetween over the Internet 14. During the dialog, the firewall 30 may provide the device 12(m) with the identification of a decryption algorithm and associated decryption key which the device 12(m) is to use in decrypting the encrypted portions of message packets which the virtual private network transmits to the device 12(m). In addition, the firewall 30 may also provide the device 12(m) with the identification of an encryption algorithm and associated encryption key which the device 12(m) is to use in encrypting the portions of message packets which the device 12(m) transmits to the virtual private network 15 which are to be encrypted; alternatively, the device 12(m) can provide the identification of the encryption algorithm

and key that it (that is device 12(m)) will use to the firewall 30 during the dialog. The device 12(m) can store in its IP parameter store 25 information concerning the secure tunnel, including information associating the identification of the firewall 30 and the identifications of the encryption and decryption algorithms and associated keys for message packets to be transferred over the secure tunnel.

Thereafter, the device 12(m) and firewall 30 can transfer message packets over the secure tunnel. The device 12(m), in generating message packets for transfer over the secure tunnel, makes use of the secure packet processor 26 to encrypt the portions of the message packets which are to be encrypted prior to transmission by the network interface 21 to the ISP 11 for transfer over the Internet 14 to the firewall 30, and to decrypt the encrypted portions of the message packets received by the device 12(m) which are encrypted. In particular, after the packet generator 22 generates a message packet for transmission to the firewall 30 over the secure tunnel, it will provide the message packet to the secure packet processor 26. The secure packet processor 26, in turn, encrypts the portions of the message packet that are to be encrypted, using the encryption algorithm and key. After the firewall 30 receives a message packet from the device 12(m) over the secure tunnel, it will decrypt it and, if the intended recipient of the message packet is another device, such as a server 31(s), in the virtual private network 14, it (that is, the firewall 30) will transfer the message packet to that other device over the communication link 33.

For a message packet that is to be transferred by a device, such as a server 31(s), in the virtual private network 15 to the device 12(m) over the secure tunnel, the firewall 30 will receive such to the message packet over the communication link 33 and encrypt the message packet for transfer over the Internet 14 to the ISP 11. The ISP 11, in turn, forwards the message packet to the device 12(m), in particular to its network interface 21. The network interface 21 provides the message packet to the secure packet processor 26, which decrypts the encrypted portions of the message packet, using the decryption algorithm and key.

A problem arises in connection with accesses by a device, such as device 12(m), which is external to the virtual private network 15, and a device, such as a server 31(s), which is external to the firewall, namely, that nameserver 17 is not provided with integer Internet addresses for servers 31(s) and other devices which are in the virtual private network 15, except for integer Internet addresses associated with the firewall 30. Thus, the device 12(m), after the operator has entered the human-readable Internet address, will not be able to obtain the integer Internet address of the server 31(s) which is to be accessed from that nameserver 17.

To accommodate this problem, when the device 12(m) and firewall 30 cooperate to establish a secure tunnel therebetween, in addition to possibly providing the device 12(m) with the identifications of the encryption and decryption algorithms and keys which are to be used in connection with the message packets transferred over the secure tunnel, the firewall 30 also provides the device 12(m) with the identification of a nameserver, such as nameserver 32, in the virtual private network 15 which the device 12(m) can access to obtain the appropriate integer Internet addresses for the human-readable Internet addresses which may be provided by the operator of device 12(m). The identification of nameserver 32 is also stored in the IP parameter store 25, along with the identification of nameserver 17 which was provided by the ISP 11 when the device 12(m) logged on to the ISP 11 at the beginning of a communications session. Thus, when the device 12(m) is to transmit a message packet to a device, such as a server 31(s) in the virtual private network 14 using a human-readable Internet address provided by, for example, an operator, the device 12(m) will initially access the nameserver 17, as described above, to attempt to obtain the integer Internet address associated with the human-readable Internet address. Since nameserver 17 is outside of the virtual private network 15 and will not have the information requested by the device 12(m), it will send a response message packet so indicating. The device 12(m) will thereafter generate a request message packet for transmission to the nameserver 32 through the firewall 30 and over the secure tunnel. If the nameserver 32 has an integer Internet address associated with the human-readable Internet address in the request message packet provided by the device 12(m), it will provide the integer Internet address in a manner that is generally similar to that described above in connection

with nameserver 18, except that the integer Internet address will be provided by the nameserver 32 in a message packet directed to the firewall 30, and the firewall 30 will thereafter transmit the message packet over the secure tunnel to the device 12(m). In the message packet transmitted by the firewall 30, it will be appreciated that the integer Internet address in the message packet will be in the data portion of the message packet transferred over the secure tunnel and, accordingly, will be in encrypted form. The message packet will be processed by the device 12(m) in a manner similar to that described above in connection with other message packets received by it over the secure tunnel, that is, the message packet will be decrypted by the secure packet processor 26 prior to being provided to the packet receiver and processor 23 for processing. The integer Internet address for the server 31(s) can be cached in an access control list ("ACL") in the IP parameter store 25, along with the association of the human-readable Internet address thereto, an indication that the server 31(s) associated with that human-readable Internet address is to be accessed through the firewall 30 of the virtual private network 15, and the identifications of the encryption and decryption algorithms and keys to be used for encrypting and decrypting the appropriate portions of the message packets transmitted to server 31(s) and received from server 31(s).

It will be appreciated that, if the nameserver 32, in response to a message packet from the device 12(m) requesting the nameserver 32 to provide an integer Internet address for a human-readable Internet address provided by the device 12(m), if the nameserver 32 does not have an association between the human-readable Internet address and an integer Internet address, the nameserver 32 can provide a response message packet so indicating. If the device 12(m) has identification of other nameservers, such as may be associated with other virtual private networks (not shown), to which it (that is, device 12(m)) may have access, then the device 12(m) can attempt to access the other nameservers in a similar manner as described above. If the device 12(m) is unable to obtain an integer Internet address associated with the human-readable Internet address from any of the nameservers to which it has access, and which generally will be identified in its IP parameter store 25, it will generally be unable to access a device having the human-readable Internet address, and may so notify its operator or program which requested the access.

With this background, operations performed by the device 12(m) and virtual private network 15 in connection with the invention will be described in detail. Generally, operations proceed in two phases. In the first phase, the device 12(m) and virtual private network 15 cooperate to establish a secure tunnel through the Internet 14. In that first phase, the virtual private network 15, in particular the firewall 30 provide the identification of a nameserver 32, and may also provide the encryption and decryption algorithm and key information, as described above. In the second phase, after the secure tunnel has been established, the device 12(m) can use the information provided during the first phase in connection with generating and transferring message packets to one or more servers 31(s) in the virtual private network 15, in the process obtaining resolution human-readable Internet addresses to integer Internet addresses as necessary from the nameserver 32 that was identified by the firewall 30 during the first phase.

Thus, in the first (secure tunnel establishment) phase, the device 12(m) initially generates a message packet requesting establishment of a secure tunnel for transfer to the firewall 30. The message packet will include an integer Internet address for the firewall (which may have been provided by the device's operator or a program being processed by the device 12(m) or have been provided by a the nameserver 17 after a human-readable Internet address was provided by the operator or a program), and which, in particular, is to enable the firewall 30 to establish secure tunnels therewith. If the firewall 30 accepts the secure tunnel establishment request, and if the firewall 30 provides the encryption and decryption algorithms and keys as noted above, it (that is, the firewall) will generate a response message packet for transmission to the device 12(m) that identifies the encryption and decryption algorithms and keys; as noted above, this response message packet will not be encrypted. When the device 12(m) receives the response message, the identifications of the encryption and decryption algorithms and keys will be stored in the IP parameter store 25.

At some point later in the first phase, the firewall 30 will also generate a message packet for transmission to the device 12(m) that includes the integer Internet address of the nameserver 32. For this message packet, the portion of the message packet that contains the integer Internet address of

the nameserver 32 will be encrypted, using encryption algorithm and key that can be decrypted using the decryption algorithm and key provided in the response message packet described above. This message will generally have a structure

```
"<IIA(FW),IIA(DEV12(m))><SEC_TUN>  
  
<ENCR<<IIA(FW),IIA(DEV_12(m))><DNS_ADRS:IIA(NS_32)>>>"
```

where

(i) "IIA(FW)" represents the source address, that is, integer Internet address of the firewall 30,

(ii) "IIA(DEV_12(m))" represents the destination address, that is, the integer Internet address of the device 12(m),

(iii) "DNS_ADRS:IIA(NS)" indicates that "IIA(NS_32)" represents the integer Internet address of the nameserver 32, the nameserver which the device 12(m) is authorized to use, and

(iv) "ENCR<...>" indicates that the information between brackets "<" and ">" is encrypted.

The initial portion of the message "<IIA(FW),IIA(DEV_12(m))>" forms at least part of the header portion of the message, and "<ENCR<<IIA(FW),IIA(DEV_12(m))><IIA(NS)>>>" represents at least part of the data portion of the message. The "<SEC_TUN>" represents an indicator in the header indicating that the message is being transferred over the secure tunnel, thereby indicating that the data portion of the message contains encrypted information.

After the device 12(m) receives the message from the firewall 30 as described above, since the message packet contains the <SEC_TUN> indicator, its network interface 21 will transfer the encrypted portion "<ENCR<<IIA(FW),IIA(DEV_12(m))><DNS_ADRS:IIA(NS_32)>>>" to the secure packet processor 26 for processing. The secure packet processor will decrypt the encrypted portion, determine that the portion "IIA(NS_32)" is the integer Internet address of a nameserver, in

particular nameserver 32, that the device 12(m) is authorized to use, and store that address in the IP parameter store 25, along with an indication that message packets thereto are to be transferred to the firewall 30 and that data in the message packets is to be encrypted using the encryption algorithm and key previously provided by the firewall 30. It will be appreciated that, since the integer Internet address of nameserver 32 is transferred from the firewall to the device 12(m) in encrypted form, it will be maintained in confidence even if the packet is intercepted by a third party.

Depending on the particular protocol used to establish the secure tunnel, the firewall 30 and device 12(m) may also exchange message packets containing other information than that described above.

As noted above, in the second phase, after the secure tunnel has been established, the device 12(m) can use the information provided during the first phase in connection with generating and transferring message packets to one or more of the servers 31(s) in the virtual private network 15. In those operations, if the operator of device 12(m), or a program being processed by device 12(m), wishes to have device 12(m) transmit a message packet to a server 31(s) in the virtual private network 15, if the operator, through the operator interface 20, or the program provides a human-readable Internet address, the device 12(m), in particular the packet generator 22, will initially determine whether the IP parameter store 25 has cached therein an integer Internet address that is associated with the human-readable Internet address. If not, the packet generator 22 will generate a request message packet for transfer to the nameserver 17 requesting it to provide the integer Internet address associated with the human-readable Internet address. If the nameserver 17 has an integer Internet address associated with the human-readable Internet address, it will provide the integer Internet address to the device 12(m). It will be appreciated that this may occur if the human-readable Internet address in the request message packet has been associated with a device 13 external to the virtual private network 15, as well as with a server 32(s) in the virtual private network 15. Thereafter, the device 12(m) can use the integer Internet address to generate message packets for transfer over the Internet as described above.

Assuming, on the other hand, that the nameserver 17 does not have a integer Internet address associated with the human-readable Internet address, it (that is, the nameserver 17) will provide a response message packet so indicating to the device 12(m). Thereafter, the packet generator 22 of device 12(m) will generate a request message packet for transmission to the next nameserver identified in its IP parameter store 25 requesting that nameserver to provide the integer Internet address associated with the human-readable Internet address. If that next nameserver is nameserver 32, the packet generator 22 will provide the message packet to the secure packet processor 26 for processing. The secure packet processor 26, in turn, will generate a request message packet for transfer over the secure tunnel to the firewall 30. This message will generally have a structure

```
"<IIA(DEV_12(m)),IIA(FW)><SEC_TUN>  
<ENCR<<IIA(DEV_12(m)),IIA(NS_32))><IIA_REQ>>>"
```

where

(i) "IIA(DEV_12(m))" represents the source address, that is, integer Internet address of the device 12(m)

(ii) "IIA(FW)" represents the destination address, that is, the integer Internet address of the firewall 30

(iii) "IIA(NS_32)" represents the address of the nameserver 32

(iii) "<<IIA(DEV_12(m)),IIA(NS_32))><IIA_REQ>>" represents the request message packet generated by the packet generator 22, where "<IIA(DEV_12(m)),IIA(NS_32)>" represents the header portion of the request message packet, and "<IIA_REQ>" represents the data portion of the request message packet,

(iv) "ENCR<....>" indicates that the information between brackets "<" and ">" is encrypted, and

(v) "<SEC_TUN>" represents an indicator in the header portion of the message packet generated by the secure packet generator 26 indicating that the message is being transferred over the secure tunnel, thereby indicating that the data portion of the message contains encrypted information.

When the firewall 30 receives the request message packet generated by the secure packet processor 26, it will decrypt the encrypted portion of the message packet to obtain <<IIA(DEV_12(m)),IIA(NS_32))>><IIA_REQ>>" represents the request message packet as generated by the packet generator 22. After obtaining the request message packet, the firewall 30 will transmit it over the communication link 33 to the nameserver 32. In that process, depending on the protocol for transmission of message packets over the communication link 33, the firewall 30 may need to modify the request message packet to conform to the protocol of communication link 33.

After the nameserver 32 receives the request message packet, it will process it to determine whether it has an integer Internet address associated with the human-readable Internet address provided in the request message packet. If the nameserver determines that it has such an integer Internet address, it will generate a response message packet including the integer Internet address for transmission to the firewall. Generally, the response message packet will have a structure:

<<IIA(NS_32),IIA(DEV_12(m))>><IIA_RESP>>

where

(i) "IIA(NS_32)" represents the source address, that is, integer Internet address of the nameserver 32,

(ii) "IIA(DEV_12(m))" represents the destination address, that is, integer Internet address of the device 12(m), and

(iii) "IIA_RESP" represents the integer Internet address associated with the human-readable Internet address.

After the firewall 30 receives the response message packet, since communications with device 12(m) are over the secure tunnel therebetween, it (that is, the firewall 30) will encrypt the response message packet received from the nameserver 32 and generate a message packet for transmission to the device 12(m) including the encrypted response message packet. Generally, the message packet generated by the firewall 30 has the structure:

```
"<IIA(FW),IIA(DEV12(m))><SEC_TUN>  
<ENCR<<IIA(NS_32),IIA(DEV_12(m))><IIA_RESP>>>"
```

where

(i) "IIA(FW)" represents the source address, that is, integer Internet address of the firewall 30,

(ii) "IIA(DEV_12(m))" represents the destination address, that is, the integer Internet address of the device 12(m),

(iii) "SEC_TUN" represents an indicator in the header portion of the message packet generated by the secure packet generator 26 indicating that the message is being transferred over the secure tunnel, thereby indicating that the data portion of the message contains encrypted information, and

(iv) "ENCR<....>" indicates that the information between brackets "<" and ">" (which constitutes the response message packet received from the nameserver 32) is encrypted.

In addition, depending on the protocol for transmission of message packets over the communication link 33, the firewall 30 may need to process and/or modify the message packet to conform to the protocol of Internet 14.

When the device 12(m) receives the message packet from the firewall 30, it (that is, the message packet) will be provided to the secure packet processor 26. The secure packet processor 26, in turn, will decrypt the encrypted portion of the message packet to obtain the integer Internet address associated with the human-readable Internet address, and load that information in the IP parameter store 25. Thereafter, the device can use that integer Internet address in generating message packets for transmission to the server 31(s) which is associated with the human-readable Internet address.

It will be appreciated that, if the nameserver 32 does not have an integer Internet address associated with the human-readable Internet address provided by the device 12(m) in the request message packet, it (that is, nameserver 32) can so indicate in the response message packet generated thereby. The firewall 30 will, in response to the response message packet provided by the nameserver 32, also generate a message packet for transmission to the device 12(m), the message packet including an encrypted portion comprising the response message packet generated by the nameserver 32. After the device 12(m) receives the message packet, the encrypted portion will be decrypted by the secure packet processor 26, which, in turn, will notify the packet generator 22 that the nameserver 32 does not have an integer Internet address associated with the human-readable Internet address. Thereafter, if the IP parameter store 25 contains the identification of another nameserver, the packet generator 22 of device 12(m) will generate a request message packet for transmission to the next nameserver identified in its IP parameter store 25 requesting that nameserver to provide the integer Internet address associated with the human-readable Internet address. On the other hand, if the IP parameter store 25 does not contain the identification of another nameserver, the packet generator 22 can notify the operator interface 20 or program that it is will be unable to generate a message packet for transmission to a device associated with the human-readable Internet address provided thereby.

An embodiment of the invention can provide a number of advantages. For example, it can provide a system for easing communications between devices connected to a public network such as the Internet 14, and devices connected to private networks such as virtual private network 15, by facilitating resolution

of human-readable addresses to network addresses by a nameservers connected to the private networks over a secure tunnel.

It will be appreciated that numerous modifications may be made to the arrangement described above in connection with FIG. 1. For example, although the network 10 has been described such that the identification of the encryption and decryption algorithms and keys are exchanged by the device 12(m) and firewall 30 during the dialog during which the secure tunnel is established, it will be appreciated that that information may be provided by the device 12(m) and firewall 30 separately from the establishment of a secure tunnel therebetween.

In addition, although an embodiment of the invention has been described in connection with the Internet, it will be appreciated that an embodiment of the invention can be used in connection with any network. Further, although an embodiment has been described in connection with a network which provides for human-readable network addresses, it will be appreciated that an embodiment can be used in connection with any network which provides for any form of secondary or informal network address arrangements.

It will be appreciated that a system in accordance with the invention can be constructed in whole or in part from special purpose hardware or a general purpose computer system, or any combination thereof, any portion of which may be controlled by a suitable program. Any program may in whole or in part comprise part of or be stored on the system in a conventional manner, or it may in whole or in part be provided in to the system over a network or other mechanism for transferring information in a conventional manner. Thus, such a computer program can form a product operable, when run on a computer, to provide the required functionality of an embodiment of the invention. The computer program product can be provided on a carrier medium, for example, a computer readable medium such as, for example, a memory, disc or other storage medium, or a transmission medium such as a telecommunications channel providing, for example, electrical, optical, wireless or other transmission. In addition, it will be appreciated that the system may be operated and/or otherwise controlled by means of information provided by an operator using operator input elements (not shown) which may be connected directly to the system or which may transfer the information to the system over a network or other mechanism for transferring information in a conventional manner.

The foregoing description has been limited to a specific embodiment of this invention. It will be apparent, however, that various variations and modifications may be made to the invention, with the attainment of some or all of the advantages of the invention.

CLAIMS

1. A system comprising a virtual private network and an external device which communicate over a digital network,

the virtual private network having a firewall, at least one internal device and a nameserver each having a network address, the internal device also having a secondary address, the nameserver being configured to provide an association between the secondary address and the network address,

the firewall, in response to a request from the external device to establish a connection therebetween, being configured to provide the external device with the network address of the nameserver, and

the external device, in response to a request requesting access to the internal device including the internal device's secondary address, being configured to generate a network address request message for transmission over the connection to the firewall requesting resolution of the network address associated with the secondary address, the firewall being configured to provide the address resolution request to the nameserver, the nameserver being configured to provide the network address associated with the secondary address, the firewall in turn being further configured to provide the network address in a network address response message for transmission over the connection to the external device.

2. A system according to claim 1, wherein the external device is further configured to use the network address provided in the network address response message in generating at least one message for transmission to the internal device.

3. A system according to claim 1 or claim 2, wherein the external device is configured to connect to the network through a network service provider.

4. A system according to claim 3, wherein the external device is configured to establish a communications session with the network service provider, the network service provider providing the external device with the identification of a further nameserver, the further nameserver being configured to provide an association between a secondary address and a network address for at least one device.

5. A system according to any preceding claim, wherein the external device is configured to maintain a list of nameservers which have been identified to said external device, the external device being configured to interrogate successive ones of the nameservers in the list in response to a request requesting access to another device, said request including a secondary address for said other device, until said external device receives a network address, in each interrogation the external device being configured to generate a said network address request message for transmission over the network for response by one of said nameservers in said list and to receive a network address response message therefrom.

6. A system according to any preceding claim, wherein the connection between the external device and the firewall is a secure tunnel, in which at least some portion of messages transferred between the external device and the firewall is encrypted.

7. A method of operating a system comprising a virtual private network and an external device interconnected by a digital network, the virtual private network having a firewall, at least one internal device and a nameserver each having a network address, the internal device also having a

secondary address, the nameserver being configured to provide an association between the secondary address and the network address, the method comprising the steps of:

- A. enabling the firewall, in response to a request from the external device to establish a connection therebetween, provide the external device with the network address of the nameserver; and
- B. enabling
 - (i) the external device, in response to a request requesting access to the internal device including the internal device's secondary address, to generate a network address request message for transmission over the connection to the firewall requesting resolution of the network address associated with the secondary address,
 - (ii) the firewall to provide the address resolution request to the nameserver,
 - (iii) the nameserver to provide the network address associated with the secondary address, and
 - (iv) the firewall to provide the network address in a network address response message for transmission over the connection to the external device.

8. A method according to claim 7, wherein the external device is further enabled to use the network address provided in the network address response message in generating at least one message for transmission to the internal device.

9. A method according to claim 7 or claim 8, wherein the external device is enabled to connect to the network through a network service provider.

10. A method according to claim 9, wherein the external device is enabled to establish a communications session with the network service provider, the network service provider being enabled to provide the external device with the identification of a further nameserver, the further nameserver being enabled to provide an association between a secondary address and a network address for at least one device.

11. A method according to any one of claims 7 to 10, wherein the external device is enabled to maintain a list of nameservers which have been identified to said external device, the external device being enabled to interrogate successive ones of the nameservers in the list in response to a request requesting access to another device, said request including a secondary address for said other device, until said external device receives a network address, in each interrogation the external device being enabled to generate a said network address request message for transmission over the network for response by one of said nameservers in said list and to receive a network address response message therefrom.

12. A method according to any one of claims 7 to 10, wherein the connection between the external device and the firewall is a secure tunnel, in which at least some portion of messages transferred between the external device and the firewall is encrypted.

13. A computer program product for use in connection with a virtual private network and an external device interconnected by a digital network, the virtual private network having a firewall, at least one internal device and a nameserver each having a network address, the internal device also having a secondary address, the nameserver being configured to provide an association between the secondary

address and the network address, the computer program product comprising :

- A. a nameserver identification code module configured to enable the firewall, in response to a request from the external device to establish a connection therebetween, to provide the external device with the network address of the nameserver,
- B. a network address request message generating code module for enabling the external device, in response to a request requesting access to the internal device including the internal device's secondary address, to generate a network address request message for transmission over the connection to the firewall requesting resolution of the network address associated with the secondary address,
- C. an address resolution request forwarding module for enabling the firewall to provide the address resolution request to the nameserver,
- D. a nameserver control module for enabling the nameserver to provide the network address associated with the secondary address, and
- E. a network address response message forwarding module for enabling the firewall to provide the network address in a network address response message for transmission over the connection to the external device.

14. A computer program product according to claim 13, further comprising a network address utilization module configured to enable the external device to use the network address provided in the network address response message in generating at least one message for transmission to the internal device.

15. A computer program product according to claim 13 or claim 14, further comprising a network service provider control module for enabling the external device to connect to the network through a network service provider.

16. A computer program product according to claim 15, wherein the network service provider control module includes a communications session establishment module for enabling the external device to a communications session with the network service provider and receive therefrom identification of a further nameserver.

17. A computer program product according to any one of claims 13 to 16, further including nameserver interrogation control module for enabling the external device to maintain a list of nameservers which have been identified to said external device, and to interrogate successive ones of the nameservers in the list in response to a request requesting access to another device, said request including a secondary address for said other device, until said external device receives a network address, in each interrogation the external device being enabled to generate a said network address request message for transmission over the network for response by one of said nameservers in said list and to receive a network address response message therefrom.

18. A computer program product according to any one of claims 13 to 16, wherein the connection between the external device and the firewall is a secure tunnel, in which at least some portion of messages transferred between the external device and the firewall is encrypted.

19. A computer program product according to any one of claims 13 to 18 on a carrier medium.
20. A computer program product according to claim 19, wherein the carrier medium is a computer readable medium.
21. A computer program product according to claim 19, wherein the carrier medium is a transmissions medium.
22. A system substantially as hereinbefore described with reference to the accompanying drawings.
23. A method substantially as hereinbefore described with reference to the accompanying drawings.
24. A computer program product substantially as hereinbefore described with reference to the accompanying drawings.



34

Application No: GB 9912200.4
Claims searched: All

Examiner: Gareth Griffiths
Date of search: 7 December 1999

**Patents Act 1977
Search Report under Section 17**

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:
UK Cl (Ed.Q): H4P (PPA, PPEB, PPEC, PPG)
Int Cl (Ed.6): H04L 12/22, 12/46, 12/66, 29/06
Other: Online Databases: WPI, EPODOC, JAPIO

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
X, P	EP0887979 A2 (SUN MICROSYSTEMS) col.15 line 35 - col.17 line 24	1, 2, 5-8, 11-14, 17-21
A	EP0825748 A2 (AT&T) col.6 line 46 - col.11 line 40	
A, P	WO98/31124 A1 (HANSON) p.5 line 2 - p.6 line 25	

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Electronic Patent Application Fee Transmittal

Application Number:	11839987
Filing Date:	16-Aug-2007
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Atabak R Royae/Melissa Molchan
Attorney Docket Number:	77580-0066 (VRNK-1 CP2DVCN)

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
Total in USD (\$)				180

Electronic Acknowledgement Receipt

EFS ID:	8152368
Application Number:	11839987
International Application Number:	
Confirmation Number:	9470
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Atabak R Royaee/Melissa Molchan
Filer Authorized By:	Atabak R Royaee
Attorney Docket Number:	77580-0066 (VRNK-1CP2DVCN)
Receipt Date:	04-AUG-2010
Filing Date:	16-AUG-2007
Time Stamp:	13:45:03
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$180
RAM confirmation Number	57
Deposit Account	501133
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	-------------------------------------	------------------	------------------

1	Information Disclosure Statement (IDS) Filed (SB/08)	0066.pdf	64096 d3e7702dcd1a710e81d53150bc876c887f67a51a	no	3
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	Foreign Reference	EP0838930A2.pdf	1724786 9a383b35683829ae78abb4965b90cde255795d93	no	34
Warnings:					
Information:					
3	Foreign Reference	EP0814589A2.pdf	1094602 10c06cd368d846b9f6c82e5622edd22ebc63e401	no	19
Warnings:					
Information:					
4	Foreign Reference	GB2317792A.pdf	1256657 d50989c41fac545a0929025d919331dfb7f136ef	no	34
Warnings:					
Information:					
5	Foreign Reference	WO9827783A1.pdf	846395 2a2ead44c192a436d19c46f7f35211b7e6ad33cf	no	23
Warnings:					
Information:					
6	Foreign Reference	WO99011019.pdf	2034462 a88bd9be7182a86a8e75ebf9a5aa6e210b0962a5	no	60
Warnings:					
Information:					
7	Foreign Reference	GB2334181A.pdf	431753 98657594c9b37568cbca8e5569b8b1bf6fd6f75a0	no	14
Warnings:					
Information:					
8	Foreign Reference	GB2340702A.pdf	1504772 b9d55f72785502abe4081ceb482776f5d62d0f15	no	36
Warnings:					
Information:					

9	NPL Documents	Baumgartner.pdf	535114	no	20
			e1cfd368a442fe0e98ec5f0b34dc39d0d51aee53		
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
10	NPL Documents	Chapman.pdf	1713700	no	19
			39c5c492b168aa3e7de9fca2a4031545bed0e957		
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
11	NPL Documents	Davila.pdf	461212	no	18
			0300df8d7b65f715e893e7e8d5e7985e93b9ed97		
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
12	NPL Documents	DeRaadt.pdf	333587	no	10
			fdad8832507203c9875d1e55fdce679b42cecc48		
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
13	NPL Documents	Eastlake.pdf	1007823	no	45
			7f990c13c14c9426828dd74c35dd10f320f607b2		
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
14	NPL Documents	Gunter.pdf	330364	no	10
			b806a4f735e709274fa23d1b659f93f2e555a2		
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
15	NPL Documents	Shimizu.pdf	1284498	no	15
			e3b8ee1a0847be8b7e6a6bc5791dafc815d3ae15		
Warnings:					

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

16	NPL Documents	Stallings.pdf	1451887	no	42
			b32ca3a1d283b7ceeadd81e075be896ce51656dd		

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

17	NPL Documents	Takata.pdf	109936	no	3
			009f8475adb2a0557fdcff79670b4a3112a0119		

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

18	NPL Documents	Wells.pdf	63145	no	1
			095ce48eaeaeaf4359dd456e88732c1e895de5e3		

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

19	Fee Worksheet (PTO-875)	fee-info.pdf	30658	no	2
			bf72fa5446f76fc924f1c70553787ba00e29a71c		

Warnings:

Information:

Total Files Size (in bytes):	16279447
-------------------------------------	----------

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

New Applications Under 35 U.S.C. 111

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

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

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

New International Application Filed with the USPTO as a Receiving Office

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Larson et al.
Application Serial No.: 11/839,987
Filing Date: August 16, 2007
Title: METHOD FOR ESTABLISHING SECURE COMMUNICATION
LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE
NETWORK
Examiner: Lim, Krisna
Art Unit: 2453
Confirmation No.: 9470
Atty. Docket No.: 077580-0066 (VRNK-1CP2DVCN2)

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

RESPONSE

In response to the non-final Office Action mailed July 8, 2010 (“the Office Action”), please amend the above-identified application as follows:

Remarks, beginning on page 2 of this paper.

Remarks

Applicant appreciates the Examiner's examination of the subject application. Claims 1-18 are currently pending.

In the Office Action, the Examiner has rejected Claims 1-18 under 35 U.S.C. § 103(a), as being unpatentable over VPN Overview and Aventail Connect v 3.1/v2.6 Administrator's Guide ("Aventail"). The Examiner rejected claims 1-18 on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 2-23 of co-pending Application No. 11/679,416.

Applicant respectfully traverses the outstanding objection and rejections and requests reconsideration of the subject application in light of the foregoing amendments and the following remarks.

Patentability under 35 U.S.C. § 103

The Examiner has rejected Claims 1-18 under 35 U.S.C. § 103(a), as being unpatentable over VPN Overview and Aventail. These rejections are respectfully traversed, and reconsideration and withdrawal of these rejections are respectfully requested.

Independent claim 1 recites the following:

A method of accessing a secure network address, comprising:

 sending a query message from a first network device to **a secure domain service**, the query message requesting from the secure domain service **a secure network address** for a second network device;

 receiving at the first network device a response message from the secure domain name service containing the secure network address for the second network device; and

 sending an access request message from the first network device to the secure network address using a **virtual private network communication link**.

(emphasis added).

As a preliminary matter, neither Aventail nor VPN Overview have been shown to be prior art to all claims in the present application, including claim 1. Aventail is not prior art because the present application claims priority to U.S. Patent Nos. 6,502,135 (hereinafter “the ‘135 patent”) and 7,188,180 (hereinafter “the ‘180 patent”). The ‘135 and ‘180 Patents have been subject to an inter partes reexamination proceedings, Control Nos. 95/001,269 (hereinafter “the ‘269 Reexam”) and 95/001,270 (hereinafter “the ‘270 Reexam”), respectively. In both Reexams, the USPTO determined that “Aventail cannot be relied upon as prior art to the [patents].” See Reexamination Control No. 95/001,269, Action Closing Prosecution, June 16, 2010, attached as Exhibit A, and Reexamination Control No. 95/001,270, Action Closing Prosecution, June 16, 2010, attached as Exhibit B. This determination was soundly based on the fact that no evidence was found that established Aventail’s publication date.

Indeed, Aventail’s identification of a copyright date range of 1996 – 1999 is not equivalent to a publication date. The distinction between a publication date and a copyright date is critical. To establish a date of publication, the reference must be shown to have “been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it.” *In re Wyre*, 655 F.2d 221 (C.C.P.A. 1981). Aventail, on its face, provides “© 1996-1999 Aventail Corporation.” The copyright date does not meet this standard. Unlike a publication date, a copyright date merely establishes “the date that the document was created or printed.” *Hilgraeve, Inc. v. Symantec Corp.*, 271 F. Supp. 2d 964, 975 (E.D. Mich. 2003).

Presuming the author of the document accurately represented the date the document was created, this creation date is not evidence of any sort of publication or dissemination. Without

more, this bald assertion of the creation of the document does not meet the “publication” standard required for a document to be relied upon as prior art.

Further exacerbating matters is the filing date of the ‘135 Patent: February 15, 2000. Suppose the relied upon sections of the Aventail reference were created on December 31, 1999, and the copyright date range were accordingly amended to read “1996-1999.” Under these circumstances, it is possible that the document, although created, was not made publicly available until after the filing date of the ‘135 Patent, six weeks after creation. Under these circumstances, Aventail clearly would not be eligible to be relied upon as prior art to the ‘135 Patent.

As an aside, the Applicant notes that the present assignee (VirnetX Inc.) and its prosecution counsel have been accused of inequitable conduct during the ‘269 Reexam in a litigation proceeding, *VirnetX Inc. v. Cisco Systems, Inc., et al.*, United States District Court for the Eastern District of Texas, Tyler Division, Case No. 6:10-cv-417. Exhibits C-E. In its Original Answer, Affirmative Defenses, and Counterclaims to the Virnetx’s Original Complaint, the Defendant Apple Inc. (“Apple”) alleges that evidence of Aventail’s publication as early as June 1999 was presented in a different trial involving Microsoft Corporation. Exhibit C at ¶ 23 (p. 14). Apple further alleges that “VirnetX was aware that the Aventail reference may have been published at least as early as June 1999.” Exhibit C at ¶ 23. Defendants Aastra Technologies Limited and Aastra USA Inc. (“Aastra”) have made similar allegations in their responsive pleadings. Exhibit D at ¶ 86 (p. 19); Exhibit E at ¶ 86 (p. 19). To the contrary, the applicants are unaware of evidence establishing Aventail’s publication date, and specifically are unaware of the June 1999 publication date alleged by Apple and Aastra in their pleadings. The trial transcript from the Microsoft trial does not discuss anything about a publication date for the

Aventail reference. Exhibit F. While the trial transcript references the Aventail product, it does not mention anything about a publication date. *See e.g.* Exhibit F-2, pp. 112, 146; Exhibit F-3, pp. 115, 119-20; Exhibit F-10 pp. 21-40; Exhibit F-11, pp. 21-32, 120-150. The deposition of Gary Tomlinson (former employee of Aventail) taken during discovery prior to the Microsoft trial is inconclusive, at best. Exhibit H at pp. 33-36. Thus, although an allegation of knowledge has been made by a third party, the applicants, the assignee and applicants' prosecution counsel have not had and do not have such knowledge. To be sure, the applicants will notify the USPTO immediately if it becomes aware of evidence of Aventail's publication date.

VPN Overview has also not been shown to be prior art. On its face, VPN Overview only provides that it was copyrighted in 1998. VPN Overview at 2. Further, the reference identifies itself as being nothing more than a draft. VPN Overview at 1 (Stating the following: "White Paper – DRAFT"). The lack of a publication date in conjunction with the document's status as a draft fail to evidence that VPN Overview is prior art to the present application.

Assuming *arguendo*, that both of these references are prior art to the present application, neither VPN Overview nor Aventail, alone or in combination, are understood to disclose or suggest the features of claim 1, particularly with respect to at least the features of "a **virtual private network** communication link," "a **secure** domain name service" and a "**secure** computer network address."

Aventail's and VPN Overview's disclosures were summarized in the Declaration of Professor Jason Nieh in support of the '270 Reexam. Reexamination Control No. 95/001,270, *Declaration of Jason Nieh, Ph.D., Pursuant to 37 C.F.R. § 1.132*, April 19, 2010, attached as Exhibit G (hereinafter "Nieh Decl."). The Nieh Decl. is cited herein to characterize the cited references and their deficiencies.

Aventail discloses a system and architecture for transmitting data between two computers using the SOCKS protocol. Nieh Decl. at ¶ 14. The system routes certain, predefined network traffic from a WinSock (Windows sockets) application to an extranet (SOCKS) server, possibly through successive servers. Aventail at 7; Nieh Decl. at ¶ 14. Upon receipt of the network traffic, the SOCKS server then transmits the network traffic to the Internet or external network. Aventail at 7; Nieh Decl. at ¶ 14. Aventail's disclosure is limited to connections created at the socket layer of the network architecture. Nieh Decl. at ¶ 14.

In operation, a component of the Aventail Connect software described in the reference resides between WinSock and the underlying TCP/IP stack. *See* Aventail at 9; Nieh Decl. at ¶ 15. The Aventail Connect software intercepts all connection requests from the user, and determines whether each request matches local, preset criteria for redirection to a SOCKS server. *See* Aventail at 10; Nieh Decl. at ¶ 15. If redirection is appropriate, then Aventail Connect creates a false DNS entry to return to the requesting application. *See* Aventail at 12; Nieh Decl. at ¶ 16. Aventail discloses that Aventail Connect then forwards the destination hostname to the extranet SOCK server over a SOCKS connection. *See* Aventail at 12; Nieh Decl. at ¶ 16. The SOCKS server performs the hostname resolution. Aventail at 12; Nieh Decl. at ¶ 17. Once the hostname is resolved, the user can transmit data over a SOCKS connection to the SOCKS server. Nieh Decl. at ¶ 17. The SOCKS server, then, separately relays that transmitted data to the target. Nieh Decl. at ¶ 17.

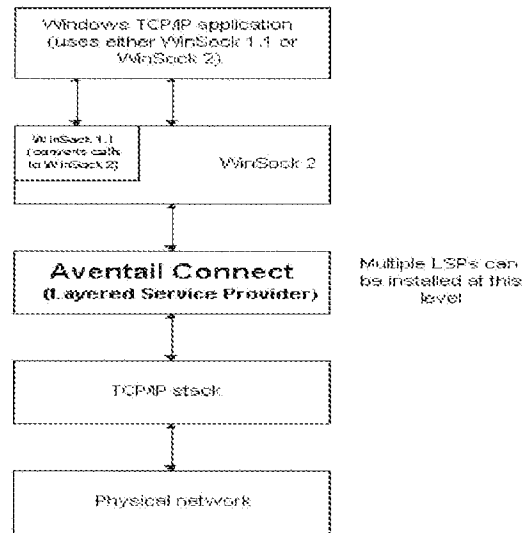
Aventail does not teach a VPN. In fact, the system disclosed in Aventail is incompatible with a VPN, and one skilled in the art would be unable to combine the two. These assertions are true for at least three reasons. First, Aventail has not been shown to demonstrate that computers connected via the Aventail system are able to communicate with each other as though they were

on the same network. *Id.* at ¶ 25. Aventail discloses establishing point-to-point SOCKS connections between a client computer and a SOCKS server. *Id.* The SOCKS server then relays data received to the intended target. *Id.* Aventail does not disclose a VPN, where data can be addressed to one or more different computers across the network, regardless of the location of the computer. *Id.*

For example, suppose two computers, A and B, reside on a public network. *Id.* at ¶ 26. Further, suppose two computers, X and Y, reside on a private network. *Id.* If A establishes a VPN connection with X and Y's network to address data to X, and B separately establishes a VPN connection with X and Y's network to address data to Y, then A would nevertheless be able to address data to B, X, and Y without additional set up. *Id.* This is true because A, B, X, and Y would all be a part of the same VPN. *Id.*

In contrast, suppose, according to Aventail, which only discloses communications at the socket layer, A establishes a SOCKS connection with a SOCKS server for relaying data to X, and B separately establishes a SOCKS connection with the SOCKS server for relaying data to Y. *Id.* at ¶ 27. In this situation, not only would A be unable to address data to Y without establishing a separate SOCKS connection (*i.e.* a VPN according to the Office Action), but A would be unable to address data to B over a secure connection. *Id.* This is one example of how the cited portions of Aventail fail to disclose a VPN. *Id.*

Second, according to Aventail, Aventail Connect's fundamental operation is incompatible with users transmitting data that are sensitive to network information. *Id.* at ¶ 28. As stated above, Aventail discloses that Aventail Connect operates between the WinSock and TCP/IP layers, as depicted on page 9:



Aventail at 9; *id.* Because Aventail discloses that Aventail Connect operates between these layers, it can intercept DNS requests. Nieh Dec. at ¶ 28. Aventail discloses that Aventail Connect intercepts certain DNS requests, and returns a false DNS response to the user if the requested hostname matches a hostname on a user-defined list. *Id.* Accordingly, Aventail discloses that the user will receive false network information from Aventail Connect for these hostnames. *Id.* If the client computer hopes to transfer to the target data that is sensitive to network information, Aventail Connect's falsification of the network information would prevent the correct transfer of data. *Id.* Aventail has not been shown to disclose a VPN.

Third, Aventail has not been shown to disclose a VPN because computers connected according to Aventail do not communicate directly with each other. *Id.* at ¶ 29. Aventail discloses a system where a client on a public network transmits data to a SOCKS server via a singular, point-to-point SOCKS connection at the socket layer of the network architecture. *Id.* The SOCKS server then relays that data to a target computer on a private network on which the SOCKS server also resides. *Id.* All communications between the client and target stop and start

at the intermediate SOCKS server. *Id.* The client cannot open a connection with the target itself. Therefore, one skilled in the art would not have considered the client and target to be virtually on the same private network. *Id.* Instead, the client computer and target computer are deliberately separated by the intermediate SOCKS server. *Id.* For these reasons, Aventail not only fails to disclose a VPN, but it discloses a system that is inherently incompatible with a VPN.

Dr. Nieh also summarized VPN Overview in his declaration. VPN Overview provides an overview of VPNs, describing their basic requirements, and some of the key technologies that permit private networking over public networks. *See*, VPN Overview at Abstract; Nieh Dec. at ¶¶ 30. As described above, Aventail is inherently incompatible with a VPN. Thus, one skilled in the art would be unable to implement the system disclosed in VPN Overview on the system disclosed in Aventail. The two references cannot be combined in the manner suggested in the Office Action of June 9, 2010, even if the references were prior art to the present application. Accordingly, VPN Overview and Aventail, either alone or in combination, are not understood to disclose, teach, or suggest the features of independent claim 1.

Moreover, neither Aventail nor VPN Overview teach or disclose “a secure domain name service” and a “secure computer network address.” Both Aventail and VPN Overview disclose conventional domain name services and computer network addresses, but not “a secure domain name” or “a secure computer network address.” *See* Office Action at 3. Indeed, in reexamination of a patent to which the current application claims priority, the Patent Office found that neither Aventail nor VPN Overview teach or disclose “a secure domain name service.” Reexamination Control No. 95/001,270, Action Closing Prosecution, June 16, 2010, attached as Exhibit B, at ¶¶ 6-7 and 9-10. (“Aventail does not teach the claimed . . . secure domain name service . . . as being a part of a non-conventional domain name system;” “VPN

Overview [does not] teach the claimed . . . secure domain name service . . . as being a part of a non-conventional domain name system.” Paragraphs [0303] – [0306] of the application also support the distinction that “a secure domain name” and “a secure computer network address” are not conventional domain name services and computer network addresses. *See also* Nieh Dec. at ¶¶ 10-13.

For all these reasons, Applicant respectfully submits that neither Aventail nor VPN Overview teach or disclose the elements of independent claim 1. Applicant respectfully submits that claim 1 is in condition for allowance. Reconsideration and withdrawal of the rejection of independent claim 1 is respectfully requested.

The other claims currently under consideration in the application are dependent from their respective independent claims discussed above and therefore are believed to be allowable over the applied references for at least the reasons provided above for their respective independent claims. Because each dependent claim is deemed to define an additional aspect of the invention, the individual consideration of each on its own merits is respectfully requested. Reconsideration and withdrawal of the rejections of the dependent claims are respectfully requested.

The absence of a reply to a specific rejection, issue, or comment does not signify agreement with or concession of that rejection, issue, or comment. In addition, because the arguments made above may not be exhaustive, there may be other reasons for patentability of any or all claims that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede, or an actual concession of, any issue with regard to any claim, or any cited art, except as specifically stated in this paper, and the amendment or cancellation of any

claim does not necessarily signify concession of unpatentability of the claim prior to its amendment or cancellation.

Non-statutory Double Patenting Rejection

Examiner has rejected claims 1-18 on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 2-23 of co-pending Application No. 11/679,416. Accordingly, Applicant submits herewith a terminal disclaimer. Applicant respectfully submits that this rejection has been overcome and requests withdrawal of this rejection.

CONCLUSION

In light of the Amendments and Remarks herein, the Applicant submits that the pending claims, claims 1-19, are in condition for allowance and respectfully requests a notice to this effect. Should the Examiner have any questions, please call the undersigned at the phone number listed below.

To the extent necessary, a petition for an extension of time (3 months) 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

/Toby H. Kusmer/

Toby H. Kusmer
Registration No. 26,418
28 State Street
Boston, MA 02109
Phone: 617-535-4065
Facsimile: 617-535-3800
Date: January 10, 2011

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

DM_US 27382961-1.077580.0066

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**TERMINAL DISCLAIMER TO OBVIATE A PROVISIONAL DOUBLE PATENTING
REJECTION OVER A PENDING "REFERENCE" APPLICATION**

Docket Number (Optional)

77580-66 (VRNK-1CP2DVCN2)

In re Application of: Larson et al.

Application No.: 11/839,987

Filed: August 16, 2007

For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

The owner*, VirnetX, of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending **reference** Application Number 11/679,416, filed on February 27, 2007, as such term is defined in 35 U.S.C. 154 and 173, and as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the **reference** application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term as defined in 35 U.S.C. 154 and 173 of any patent granted on said **reference** application, "as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application," in the event that: any such patent: granted on the pending **reference** application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

Check either box 1 or 2 below, if appropriate.

1. For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

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

2. The undersigned is an attorney or agent of record. Reg. No. 26,418

/Toby H. Kusmer/
Signature

January 10, 2011
Date

Toby H. Kusmer
Typed or printed name

617-535-4000
Telephone Number

- Terminal disclaimer fee under 37 CFR 1.20(d) is included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this statement. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Privacy Act Statement

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

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

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

Electronic Patent Application Fee Transmittal

Application Number:	11839987
Filing Date:	16-Aug-2007
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Toby H. Kusmer./Kelly Ciarmataro
Attorney Docket Number:	77580-0066 (VRNK-1 CP2DVCN)

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:				
Extension - 3 months with \$0 paid	1253	1	1110	1110

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Statutory or terminal disclaimer	1814	1	140	140
Total in USD (\$)				1250

Electronic Acknowledgement Receipt

EFS ID:	9200687
Application Number:	11839987
International Application Number:	
Confirmation Number:	9470
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kelly Ciarmataro
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-0066 (VRNK-1CP2DVCN)
Receipt Date:	10-JAN-2011
Filing Date:	16-AUG-2007
Time Stamp:	16:52:07
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$1250
RAM confirmation Number	3609
Deposit Account	501133
Authorized User	

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

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

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

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	Amendment.pdf	268500 7975d6480a79415cd324718920d46e6d1e11c1c	no	12

Warnings:

Information:

2	Terminal Disclaimer Filed	TermDisc.pdf	207217 2acc803c600ae63779c1a0c26b9e971641f19130	no	2
---	---------------------------	--------------	--	----	---

Warnings:

Information:

3	Fee Worksheet (PTO-875)	fee-info.pdf	32601 d7de7b44afd3ee2798d1bd03b9c8305bbc b2235b	no	2
---	-------------------------	--------------	--	----	---

Warnings:

Information:

Total Files Size (in bytes):

508318

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.

EXHIBIT A



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/001,269	12/08/2009	6502135	77580-89	2038

23630 7590 06/16/2010
McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

EXAMINER

NALVEN, ANDREW L

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
06/16/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O.Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS
ROTHWELL, FIGG, ERNST & MANBECK, P.C.
1425 K STREET N.W.
SUITE 800
WASHINGTON, D.C.

Date: **MAILED**

JUN 16 2010

CENTRAL REEXAMINATION UNIT

**Transmittal of Communication to Third Party Requester
Inter Partes Reexamination**

REEXAMINATION CONTROL NO. : 95001269
PATENT NO. : 6502135
TECHNOLOGY CENTER : 3999
ART UNIT : 3992

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified Reexamination proceeding. 37 CFR 1.903.

Prior to the filing of a Notice of Appeal, each time the patent owner responds to this communication, the third party requester of the inter partes reexamination may once file written comments within a period of 30 days from the date of service of the patent owner's response. This 30-day time period is statutory (35 U.S.C. 314(b)(2)), and, as such, it cannot be extended. See also 37 CFR 1.947.

If an ex parte reexamination has been merged with the inter partes reexamination, no responsive submission by any ex parte third party requester is permitted.

All correspondence relating to this inter partes reexamination proceeding should be directed to the Central Reexamination Unit at the mail, FAX, or hand-carry addresses given at the end of the communication enclosed with this transmittal.

PTOL-2070(Rev.07-04)

ACTION CLOSING PROSECUTION (37 CFR 1.949)	Control No.	Patent Under Reexamination	
	95/001,269	6502135	
	Examiner	Art Unit	
	ANDREW L. NALVEN	3992	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

Responsive to the communication(s) filed by:

Patent Owner on 15 April 2010
Third Party(ies) on 18 May 2010

Patent owner may once file a submission under 37 CFR 1.951(a) within 1 month(s) from the mailing date of this Office action. Where a submission is filed, third party requester may file responsive comments under 37 CFR 1.951(b) within 30-days (not extendable- 35 U.S.C. § 314(b)(2)) from the date of service of the initial submission on the requester. **Appeal cannot be taken from this action.** Appeal can only be taken from a Right of Appeal Notice under 37 CFR 1.953.

All correspondence relating to this inter partes reexamination proceeding should be directed to the **Central Reexamination Unit** at the mail, FAX, or hand-carry addresses given at the end of this Office action.

PART I. THE FOLLOWING ATTACHMENT(S) ARE PART OF THIS ACTION:

1. Notice of References Cited by Examiner, PTO-892
2. Information Disclosure Citation, PTO/SB/08
3. _____

PART II. SUMMARY OF ACTION:

- 1a. Claims 1-10,12 and 18 are subject to reexamination.
- 1b. Claims _____ are not subject to reexamination.
2. Claims _____ have been canceled.
3. Claims 1-10 and 12 are confirmed. [Unamended patent claims]
4. Claims 18 are patentable. [Amended or new claims]
5. Claims _____ are rejected.
6. Claims _____ are objected to.
7. The drawings filed on _____ are acceptable are not acceptable.
8. The drawing correction request filed on _____ is: approved. disapproved.
9. Acknowledgment is made of the claim for priority under 35 U.S.C. 119 (a)-(d). The certified copy has:
 been received. not been received. been filed in Application/Control No _____
10. Other _____

ACTION CLOSING PROSECUTION

This Action Closing Prosecution is responsive to the amendment and arguments filed by the patent owner on April 15, 2010 and the notice of non-participation filed by Third Party Requestor on May 18, 2010.

Receipt of Papers

1. On April 15, 2010, Patent Owner filed a response to the 1/15/2010 office action.
2. On May 18, 2010, Third Party Requestor ("Requestor") filed a notice of non-participation in the present *inter partes* reexamination. The notice indicated that no response to the 1/15/2010 office action would be submitted by the Requestor and that the Requestor will not be further participating in this proceeding.

Rejections Proposed by Requestor – Previously Adopted, Now Not Adopted

3. Requestor proposed that claims 1, 3, 4, 6-10 and 12 be rejected under 35 US C 102(a) as being anticipated by Aventail. This proposed rejection was adopted in the first Office action mailed on 1/15/2010. However, upon consideration of the remarks submitted by Patent Owner, this proposed rejection is hereby withdrawn and not adopted for the following reasons.
4. Patent owner argues that the rejection of claims 1, 3, 4, 6-10, and 12 as anticipated by Aventail should be withdrawn because Aventail is not prior art to the patent under reexamination, US Patent No. 6,502,135 ("the '135 patent"). Specifically, Patent Owner argued that the request and the 1/15/2010 office action did not show that Aventail was published prior to the priority date of the '135 patent. The request asserts that Aventail was published between

Art Unit: 3992

1996 and 1999. This assertion was based on the document's copyright date. The request did not set forth any further evidence of the date of publication.

5. A search was conducted to determine the publication date of the Aventail reference. However, no evidence was found that established the publication date. Accordingly, Aventail cannot be relied upon as prior art to the '135 patent and all rejections based upon Aventail are hereby withdrawn and not adopted.

Rejections Proposed by Requestor – Previously Not Adopted That Remain Not Adopted

6. The non-final action mailed on January 15, 2010 is hereby incorporated by reference.

7. Requestor proposed that claims 2 and 5 be rejected under 35 US C 102(a) as being anticipated by Aventail. This proposed rejection was not adopted for the reasons set forth on Pages 9-12 of the January 15, 2010 non-final office action.

8. Requestor proposed that claims 1-10 and 12 be rejected under 35 US C 102(b) as being anticipated by Kosiuer. This proposed rejection was not adopted for the reasons set forth on Pages 12-14 of the January 15, 2010 non-final office action.

9. Requestor proposed that claims 3, 6; and 8 be rejected under 35 US C 103(a) as being rendered obvious by VPN Overview in view of Aventail. This proposed rejection was not adopted for the reasons set forth on Page 14 of the January 15, 2010 non-final office action.

STATEMENT OF REASONS FOR PATENTABILITY AND/OR CONFIRMATION

Art Unit: 3992

The following is an examiner's statement of reasons for patentability and/or confirmation of the claims found patentable in this reexamination proceeding:

Claims 1, 3, 4, 6-10, 12, and 18 are confirmed as patentable for the following reasons. As noted above, Aventail is not prior art to the '135 patent. Accordingly, the remaining cited prior art includes the Gauntlet, Kosiur, Microsoft VPN, VPN Overview, and RFC 1035 references. These references do not anticipate or render obvious claims 1, 3, 4, 6-10, 12, and 18 because they fail to teach or suggest the feature of "in response to determining that the DNS request in step (2) is requesting access to a secure target web site, automatically initiating the VPN between the client computer and the target computer" as set forth in claim 1 and similarly set forth in claims 10 and 18.

Claims 2 and 5 are confirmed as patentable for the reasons set forth in the January 15, 2010 non-final office action on pages 10-12. New claim 18 is further confirmed as patentable because of its inclusion of the subject matter of claims 2 and 5.

Any comments considered necessary by the PATENT OWNER regarding the above statement must be submitted promptly to avoid processing delays. Such submission by the patent owner should be labeled: "Comments on Statement of Reasons for Patentability and/or Confirmation" and will be placed in the reexamination file.

ACTION CLOSING PROSECUTION

This is an ACTION CLOSING PROSECUTION (ACP); see MPEP § 2671.02.

(1) Pursuant to 37 CFR 1.951(a), the patent owner may once file written comments limited to the issues raised in the reexamination proceeding and/or present a proposed amendment to the claims which amendment will be subject to the criteria of 37 CFR 1.116 as to whether it shall be entered and considered. Such comments and/or proposed amendments must

Art Unit: 3992

be filed within a time period of 30 days or one month (whichever is longer) from the mailing date of this action. Where the patent owner files such comments and/or a proposed amendment, the third party requester may once file comments under 37 CFR 1.951(b) responding to the patent owner's submission within 30 days from the date of service of the patent owner's submission on the third party requester.

(2) If the patent owner does not timely file comments and/or a proposed amendment pursuant to 37 CFR 1.951(a), then the third party requester is precluded from filing comments under 37 CFR 1.951(b).

(3) Appeal **cannot** be taken from this action, since it is not a final Office action.

All correspondence relating to this *inter partes* reexamination proceeding should be directed:

By Mail to: Mail Stop *Inter Partes* Reexam
Attn: Central Reexamination Unit
Commissioner of Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to: (571) 273-9900
Central Reexamination Unit

By hand: Customer Service Window
Randolph Building
401 Dulany St.
Alexandria, VA 22314

Any inquiry concerning this communication or earlier communications from the examiner, or as to the status of this proceeding, should be directed to the Central Reexamination Unit at telephone number (571) 272-7705.

Signed:

/Andrew Nalven/

Andrew Nalven
CRU Examiner
GAU 3992
(571) 272-3839

Conferee: ESK

Conferee: JOT

EXHIBIT B



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/001,270	12/08/2009	7188180	077580-0090	2128

23630 7590 06/16/2010
McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

EXAMINER

NALVEN, ANDREW L

ART UNIT PAPER NUMBER

3992

MAIL DATE DELIVERY MODE

06/16/2010

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patents and Trademark Office
P.O.Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS
ROTHWELL, FIGG, ERNST & MANBECK, P.C.
1425 K STREET N.W.
SUITE 800
WASHINGTON, D.C. 20005

Date:

MAILED

JUN 16 2010

CENTRAL REEXAMINATION UNIT

**Transmittal of Communication to Third Party Requester
Inter Partes Reexamination**

REEXAMINATION CONTROL NO. : 95001270
PATENT NO. : 7188180
TECHNOLOGY CENTER : 3999
ART UNIT : 3992

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified Reexamination proceeding. 37 CFR 1.903.

Prior to the filing of a Notice of Appeal, each time the patent owner responds to this communication, the third party requester of the inter partes reexamination may once file written comments within a period of 30 days from the date of service of the patent owner's response. This 30-day time period is statutory (35 U.S.C. 314(b)(2)), and, as such, it cannot be extended. See also 37 CFR 1.947.

If an ex parte reexamination has been merged with the inter partes reexamination, no responsive submission by any ex parte third party requester is permitted.

All correspondence relating to this inter partes reexamination proceeding should be directed to the Central Reexamination Unit at the mail, FAX, or hand-carry addresses given at the end of the communication enclosed with this transmittal.

PTOL-2070(Rev.07-04)

ACTION CLOSING PROSECUTION (37 CFR 1.949)	Control No.	Patent Under Reexamination	
	95/001,270	7188180	
	Examiner	Art Unit	
	ANDREW L. NALVEN	3992	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

Responsive to the communication(s) filed by:

Patent Owner on 19 April 2010
 Third Party(ies) on 18 May 2010

Patent owner may once file a submission under 37 CFR 1.951(a) within 1 month(s) from the mailing date of this Office action. Where a submission is filed, third party requester may file responsive comments under 37 CFR 1.951(b) within 30-days (not extendable- 35 U.S.C. § 314(b)(2)) from the date of service of the initial submission on the requester. **Appeal cannot be taken from this action.** Appeal can only be taken from a Right of Appeal Notice under 37 CFR 1.953.

All correspondence relating to this inter partes reexamination proceeding should be directed to the **Central Reexamination Unit** at the mail, FAX, or hand-carry addresses given at the end of this Office action.

PART I. THE FOLLOWING ATTACHMENT(S) ARE PART OF THIS ACTION:

1. Notice of References Cited by Examiner, PTO-892
2. Information Disclosure Citation, PTO/SB/08
3. _____

PART II. SUMMARY OF ACTION:

- 1a. Claims 1,4,10,12-15,17,20,26,28-31,33 and 35 are subject to reexamination.
- 1b. Claims 2,3,5-9,11,16,18,19,21-25,27,32,34 and 36-41 are not subject to reexamination.
2. Claims _____ have been canceled.
3. Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are confirmed. [Unamended patent claims]
4. Claims _____ are patentable. [Amended or new claims]
5. Claims _____ are rejected.
6. Claims _____ are objected to.
7. The drawings filed on _____ are acceptable are not acceptable.
8. The drawing correction request filed on _____ is: approved. disapproved.
9. Acknowledgment is made of the claim for priority under 35 U.S.C. 119 (a)-(d). The certified copy has:
 been received. not been received. been filed in Application/Control No _____
10. Other _____

ACTION CLOSING PROSECUTION

This Action Closing Prosecution is responsive to the amendment and arguments filed by the patent owner on April 19, 2010 and the notice of non-participation filed by Third Party Requestor on May 18, 2010.

Receipt of Papers

1. On April 19, 2010, Patent Owner filed a response to the 1/19/2010 office action.
2. On May 18, 2010, Third Party Requestor ("Requestor") filed a notice of non-participation in the present *inter partes* reexamination. The notice indicated that no response to the 1/19/2010 office action would be submitted by the Requestor and that the Requestor will not be further participating in this proceeding.

Rejections Proposed by Requestor – Previously Adopted, Now Not Adopted

3. Requestor proposed that claims 1, 10, 12, 14, 17, 26, 28, 30, 31, and 33 be rejected under 35 US C 102(a) as being anticipated by Aventail. This proposed rejection was adopted in the first Office action mailed on 1/19/2010. However, upon consideration of the remarks submitted by Patent Owner, this proposed rejection is hereby withdrawn and not adopted for the following reasons.
4. Patent owner argues that the rejection of claims 1, 10, 12, 14, 17, 26, 28, 30, 31, and 33 as anticipated by Aventail should be withdrawn because Aventail is not prior art to the patent under reexamination, US Patent No. 7,188,180 ("the '180 patent"). Specifically, Patent Owner argued that the request and the 1/19/2010 office action did not show that Aventail was published

Art Unit: 3992

prior to the priority date of the '180 patent. The request asserts that Aventail was published between 1996 and 1999. This assertion was based on the document's copyright date. The request did not set forth any further evidence of the date of publication.

5. A search was conducted to determine the publication date of the Aventail reference. However, no evidence was found that established the publication date. Accordingly, Aventail cannot be relied upon as prior art to the '180 patent and all rejections based upon Aventail are hereby withdrawn and not adopted.

6. Further, Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name" from a domain name that happens to correspond to a secure computer. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name." For example, the '180 patent explains that a secure domain name is a non-standard domain name and that querying a convention domain name server using a secure domain name will result in a return message indicating that the URL is unknown (*'180 patent, column 51 lines 25-35*). Similarly, Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name service" from a conventional domain name service that can resolve domain names of computers that are used to establish secure connections. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name service." For example, the '180 patent explains that a secure domain name service can resolve addresses for a secure domain name whereas a conventional domain name service cannot resolve addresses for a secure domain name (*'180 patent, column 51 lines 25-35*).

Art Unit: 3992

7. Aventail does not teach the claimed "secure domain name" or "secure domain name service" as defined by the '180 patent. Aventail teaches the use of a DNS server and the creation of a secure tunnel to a secure remote site. However, Aventail does not teach the claimed secure domain name or secure domain name service as defined by the '180 patent as being a part of a non-conventional domain name system. For this additional reason the proposed rejection is not adopted.

8. Requestor proposed that claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 be rejected under 35 USC 103(a) as being rendered obvious by the combination of VPN Overview in view of RFC 1035. This proposed rejection was adopted in the first Office action mailed on 1/19/2010. However, upon consideration of the remarks submitted by Patent Owner, this proposed rejection is hereby withdrawn and not adopted for the following reasons.

9. Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name" from a domain name that happens to correspond to a secure computer. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name." For example, the '180 patent explains that a secure domain name is a non-standard domain name and that querying a convention domain name server using a secure domain name will result in a return message indicating that the URL is unknown (*'180 patent, column 51 lines 25-35*). Similarly, Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name service" from a conventional domain name service that can resolve domain names of computers that are used to establish secure connections. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent

Art Unit: 3992

distinguishes the claimed "secure domain name service." For example, the '180 patent explains that a secure domain name service can resolve addresses for a secure domain name whereas a conventional domain name service cannot resolve addresses for a secure domain name (*'180 patent, column 51 lines 25-35*).

10. VPN Overview and RFC 1035 do not teach the claimed "secure domain name" or "secure domain name service" as defined by the '180 patent. RFC 1035 describes the framework for a conventional domain name system (*RFC 1035, Page 3*), but does not disclose an implementation including a secure domain name service and secure domain names as claimed by the '180 patent. Similarly, VPN Overview provides an overview of virtual private networks including their basic requirements. However, neither RFC 1035 or VPN Overview teach the claimed secure domain name or secure domain name service as defined by the '180 patent as being a part of a non-conventional domain name system. Accordingly, the proposed rejection is not adopted.

11. Requestor proposed that claims 1, 10, 12-15, 17, 26, 28-31, and 33 be rejected under 35 USC 102(a) as being anticipated by Kaufman. This proposed rejection was adopted in the first Office action mailed on 1/19/2010. However, upon consideration of the remarks submitted by Patent Owner, this proposed rejection is hereby withdrawn and not adopted for the following reasons.

12. Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name" from a domain name that happens to correspond to a secure computer. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name." For example, the '180 patent explains that a secure domain

Art Unit: 3992

name is a non-standard domain name and that querying a convention domain name server using a secure domain name will result in a return message indicating that the URL is unknown (*'180 patent, column 51 lines 25-35*). Similarly, Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name service" from a conventional domain name service that can resolve domain names of computers that are used to establish secure connections. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name service." For example, the '180 patent explains that a secure domain name service can resolve addresses for a secure domain name whereas a conventional domain name service cannot resolve addresses for a secure domain name (*'180 patent, column 51 lines 25-35*).

13. Kaufman does not teach the claimed "secure domain name" or "secure domain name service" as defined by the '180 patent. Kaufman describes the implementation of virtual private networks and IPsec security, but does not disclose an implementation including a secure domain name service and secure domain names as claimed by the '180 patent. Kaufman does not teach the claimed secure domain name or secure domain name service as defined by the '180 patent as being a part of a non-conventional domain name system. Accordingly, the proposed rejection is not adopted.

14. Requestor proposed that claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 be rejected under 35 USC 103(a) as being rendered obvious by the combination of Kaufman in view of Galvin. This proposed rejection was adopted in the first Office action mailed on 1/19/2010.

Art Unit: 3992

However, upon consideration of the remarks submitted by Patent Owner, this proposed rejection is hereby withdrawn and not adopted for the following reasons.

15. Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name" from a domain name that happens to correspond to a secure computer. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name." For example, the '180 patent explains that a secure domain name is a non-standard domain name and that querying a convention domain name server using a secure domain name will result in a return message indicating that the URL is unknown (*'180 patent, column 51 lines 25-35*). Similarly, Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name service" from a conventional domain name service that can resolve domain names of computers that are used to establish secure connections. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name service." For example, the '180 patent explains that a secure domain name service can resolve addresses for a secure domain name whereas a conventional domain name service cannot resolve addresses for a secure domain name (*'180 patent, column 51 lines 25-35*).

16. Kaufman and Galvin do not teach the claimed "secure domain name" or "secure domain name service" as defined by the '180 patent. Kaufman describes the implementation of virtual private networks and IPsec security, but does not disclose an implementation including a secure domain name service and secure domain names as claimed by the '180 patent. Galvin describes a domain name service that uses public keys to prove the integrity of a domain name service record (*Galvin, Page 1*). However, this type of domain name service is a conventional type of

Art Unit: 3992

domain name service that is different from the claimed secure domain name service because it still relies on conventional domain names and does not provide security for secure domains. Instead, it seeks to prove the authenticity of a domain name service record to prove to a client that that the record was not forged. Kaufman and Galvin do not teach the claimed secure domain name or secure domain name service as defined by the '180 patent as being a part of a non-conventional domain name system. Accordingly, the proposed rejection is not adopted.

17. Requestor proposed that claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 be rejected under 35 USC 102(a) as being anticipated by Gauntlet. This proposed rejection was adopted in the first Office action mailed on 1/19/2010. However, upon consideration of the remarks submitted by Patent Owner, this proposed rejection is hereby withdrawn and not adopted for the following reasons.

18. Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name" from a domain name that happens to correspond to a secure computer. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name." For example, the '180 patent explains that a secure domain name is a non-standard domain name and that querying a convention domain name server using a secure domain name will result in a return message indicating that the URL is unknown (*'180 patent, column 51 lines 25-35*). Similarly, Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name service" from a conventional domain name service that can resolve domain names of computers that are used to establish secure connections. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent

Art Unit: 3992

distinguishes the claimed "secure domain name service." For example, the '180 patent explains that a secure domain name service can resolve addresses for a secure domain name whereas a conventional domain name service cannot resolve addresses for a secure domain name (*'180 patent, column 51 lines 25-35*).

19. Gauntlet does not teach the claimed "secure domain name" or "secure domain name service" as defined by the '180 patent. Gauntlet describes the implementation of a software based firewall system that provides for tunneling where the addresses of the secure tunneling servers must be advertised, but does not disclose an implementation including a secure domain name service and secure domain names as claimed by the '180 patent. Gauntlet does not teach the claimed secure domain name or secure domain name service as defined by the '180 patent as being a part of a non-conventional domain name system. Accordingly, the proposed rejection is not adopted.

20. Requestor proposed that claims 1, 4, 10, 12-15, 17, 26, 28-31, 33, and 35 be rejected under 35 USC 103(a) as being rendered obvious by the combination of Hands-On in view of Installing NT. This proposed rejection was adopted in the first Office action mailed on 1/19/2010. However, upon consideration of the remarks submitted by Patent Owner, this proposed rejection is hereby withdrawn and not adopted for the following reasons.

21. Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name" from a domain name that happens to correspond to a secure computer. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name." For example, the '180 patent explains that a secure domain

Art Unit: 3992

name is a non-standard domain name and that querying a convention domain name server using a secure domain name will result in a return message indicating that the URL is unknown (*'180 patent, column 51 lines 25-35*). Similarly, Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name service" from a conventional domain name service that can resolve domain names of computers that are used to establish secure connections. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name service." For example, the '180 patent explains that a secure domain name service can resolve addresses for a secure domain name whereas a conventional domain name service cannot resolve addresses for a secure domain name (*'180 patent, column 51 lines 25-35*).

22. Hands-On and Installing NT do not teach the claimed "secure domain name" or "secure domain name service" as defined by the '180 patent. Hands-On describes the implementation of secure communications using PPTP tunneling protocols and describes the use of a conventional DNS system, but does not disclose an implementation including a secure domain name service and secure domain names as claimed by the '180 patent. Installing NT describes the use of a PPTP server to set up a secure connection, but does not describe the use of a secure domain name service using a secure domain name. Hands-On and Installing NT do not teach the claimed secure domain name or secure domain name service as defined by the '180 patent as being a part of a non-conventional domain name system. Accordingly, the proposed rejection is not adopted.

Art Unit: 3992

23. Requestor proposed that claims 1, 10, 12-15, 17, 26, 28-31, and 33 be rejected under 35 USC 102(a) as being anticipated by Microsoft VPN. This proposed rejection was adopted in the first Office action mailed on 1/19/2010. However, upon consideration of the remarks submitted by Patent Owner, this proposed rejection is hereby withdrawn and not adopted for the following reasons.

24. Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name" from a domain name that happens to correspond to a secure computer. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name." For example, the '180 patent explains that a secure domain name is a non-standard domain name and that querying a convention domain name server using a secure domain name will result in a return message indicating that the URL is unknown (*'180 patent, column 51 lines 25-35*). Similarly, Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name service" from a conventional domain name service that can resolve domain names of computers that are used to establish secure connections. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name service." For example, the '180 patent explains that a secure domain name service can resolve addresses for a secure domain name whereas a conventional domain name service cannot resolve addresses for a secure domain name (*'180 patent, column 51 lines 25-35*).

25. Microsoft VPN does not teach the claimed "secure domain name" or "secure domain name service" as defined by the '180 patent. Microsoft VPN describes the implementation of a virtual private network to allow a remote client to gain access to a corporate network using a

Art Unit: 3992

PPTP tunnel through a VPN server, but does not disclose an implementation including a secure domain name service and secure domain names as claimed by the '180 patent. Microsoft VPN does not teach the claimed secure domain name or secure domain name service as defined by the '180 patent as being a part of a non-conventional domain name system. Accordingly, the proposed rejection is not adopted.

Rejections Proposed by Requestor – Previously Not Adopted That Remain Not Adopted

26. The non-final action mailed on January 19, 2010 is hereby incorporated by reference.

27. Requestor proposed that claims 4, 13, 15, 20, 29, 31, and 35 be rejected under 35 USC 102(a) as being anticipated by Aventail. This proposed rejection was not adopted for the reasons set forth on Pages 12-15 of the January 19, 2010 non-final office action.

28. Requestor proposed that claims 4, 20, and 35 be rejected under 35 USC 103(a) as being rendered obvious by the combination of VPN Overview in view of RFC 1035. This proposed rejection was not adopted for the reasons set forth on Pages 16-17 of the January 19, 2010 non-final office action.

29. Requestor proposed that claims 4, 20, and 35 be rejected under 35 USC 102(a) as being anticipated by Kaufman. This proposed rejection was not adopted for the reasons set forth on Pages 20-21 of the January 19, 2010 non-final office action.

30. Requestor proposed that claims 4, 20, and 35 be rejected under 35 USC 103(a) as being rendered obvious by the combination of Kaufman in view of Galvin. This proposed rejection

Art Unit: 3992

was not adopted for the reasons set forth on Pages 22-23 of the January 19, 2010 non-final office action.

31. Requestor proposed that claims 4, 20, and 35 be rejected under 35 USC 102(a) as being anticipated by Gauntlet. This proposed rejection was not adopted for the reasons set forth on Page 24 of the January 19, 2010 non-final office action.

32. Requestor proposed that claims 4, 20, and 35 be rejected under 35 USC 103(a) as being rendered obvious by the combination of Hands-On in view of Installing NT. This proposed rejection was not adopted for the reasons set forth on Pages 25-26 of the January 19, 2010 non-final office action.

STATEMENT OF REASONS FOR PATENTABILITY AND/OR CONFIRMATION

The following is an examiner's statement of reasons for patentability and/or confirmation of the claims found patentable in this reexamination proceeding:

Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are confirmed as patentable for the following reasons. The cited prior art fails to teach or suggest the claimed features of a "secure domain name" and a "secure domain name service." Instead, the cited prior art teaches the use of a conventional domain name system and conventional domain names where some of the domain names correspond to a host that requires authentication. The '180 patent distinguishes the claimed secure domain names and secure domain name service from a conventional domain name service by explaining that a secure domain name is a non-standard domain name and that querying a conventional domain name server using a secure domain name will result in a return

Art Unit: 3992

message indicating that the URL is unknown ('180 patent, column 51 lines 25-35) and that a secure domain name service can resolve addresses for a secure domain name whereas a conventional domain name service cannot resolve addresses for a secure domain name ('180 patent, column 51 lines 25-35). Accordingly, the cited prior art fails to anticipate or render obvious claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35.

Any comments considered necessary by the PATENT OWNER regarding the above statement must be submitted promptly to avoid processing delays. Such submission by the patent owner should be labeled: "Comments on Statement of Reasons for Patentability and/or Confirmation" and will be placed in the reexamination file.

ACTION CLOSING PROSECUTION

This is an ACTION CLOSING PROSECUTION (ACP); see MPEP § 2671.02.

(1) Pursuant to 37 CFR 1.951(a), the patent owner may once file written comments limited to the issues raised in the reexamination proceeding and/or present a proposed amendment to the claims which amendment will be subject to the criteria of 37 CFR 1.116 as to whether it shall be entered and considered. Such comments and/or proposed amendments must be filed within a time period of 30 days or one month (whichever is longer) from the mailing date of this action. Where the patent owner files such comments and/or a proposed amendment, the third party requester may once file comments under 37 CFR 1.951(b) responding to the patent owner's submission within 30 days from the date of service of the patent owner's submission on the third party requester.

(2) If the patent owner does not timely file comments and/or a proposed amendment pursuant to 37 CFR 1.951(a), then the third party requester is precluded from filing comments under 37 CFR 1.951(b).

(3) Appeal **cannot** be taken from this action, since it is not a final Office action.

All correspondence relating to this *inter partes* reexamination proceeding should be directed:

By Mail to: Mail Stop *Inter Partes* Reexam
Attn: Central Reexamination Unit

Application/Control Number: 95/001,270

Page 15

Art Unit: 3992

Commissioner of Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to: (571) 273-9900
Central Reexamination Unit

By hand: Customer Service Window
Randolph Building
401 Dulany St.
Alexandria, VA 22314

Any inquiry concerning this communication or earlier communications from the examiner, or as to the status of this proceeding, should be directed to the Central Reexamination Unit at telephone number (571) 272-7705.

Signed:

/Andrew Nalven/

Andrew Nalven
CRU Examiner
GAU 3992
(571) 272-3839

Conferee: ESK

Conferee: AT

Subst. for form 1449/PTO

Complete if Known

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

Application Number	95/001,270
Filing Date	12-08-2009
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Andrew L. Nalven
Docket Number	007580-0090

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
AN	A1	5,764,906	06/1998	Edelstein et al.	
	A2	5,864,666	01/1999	Shrader, Theodore Jack London	
	A3	5,898,830	04/1999	Wesinger et al.	
	A4	6,052,788	04/2000	Wesinger et al.	
	A5	6,061,346	05/2000	Nordman, Mikael	
	A6	6,081,900	06/2000	Subramaniam et al.	
	A7	6,101,182	08/2000	Sistanizadeh et al.	
	A8	6,199,112	03/2001	Wilson, Stephen K.	
	A9	6,202,081	03/2001	Naudus, Stanley T.	
	A10	6,298,341	10/2001	Mann et al.	
	A11	6,262,987	07/2001	Mogul, Jeffrey C.	
	A12	6,314,463	11/2001	Abbott et al.	
	A13	6,338,082	01/2002	Schneider, Eric	
	A14	6,502,135	12/2002	Munger et al.	
	A15	6,557,037	04/2003	Provino, Joseph E.	
	A16	6,687,746	02/2004	Shuster et al.	
	A17	6,757,740	06/2004	Parkh et al.	
	A18	7,039,713	05/2006	Van Gunter et al.	
	A19	7,167,904	01/2007	Devarajan et al.	
	A20	7,188,175	03/2007	McKeeth, James A.	
	A21	7,461,334	12/2008	Lu et al.	
	A22	7,490,151	02/2009	Munger et al.	
	A23	7,493,403	02/2009	Shull et al.	

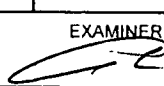
U.S. PATENT APPLICATION PUBLICATIONS

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
AN	B1	US2001/0049741	12/2001	Skene et al.	
	B2	US2004/0199493	10/2004	Ruiz et al.	
	B3	US2004/0199520	10/2004	Ruiz et al.	
	B4	US2004/0199608	10/2004	Rechterman et al.	
	B5	US2004/0199620	10/2004	Ruiz et al.	
	B6	US2007/0208869	09/2007	Adelman et al.	
	B7	US2007/0214284	09/2007	King et al.	

Subst. for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Application Number	95/001,270
				Filing Date	12-08-2009
				First Named Inventor	Victor Larson
				Art Unit	3992
				Examiner Name	Andrew L. Nalven
				Docket Number	007580-0090

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
AN	B8	US2007/0266141	11/2007	Norton, Michael Anthony	
AN	B9	US2008/0235507	09/2008	Ishikawa et al.	

FOREIGN PATENT DOCUMENTS							
EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes - Number - Kind Codes (if known)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No
AN ↓	C1	JP04-363941	12/16/1992	Nippon Telegr & Teleph Corp		English Abstract	
	C2	JP09-018492	01/17/1997	Nippon Telegr & Teleph Corp		English Abstract	
	C3	JP10-070531	03/10/1998	Brother Ind Ltd.		English Abstract	
	C4	JP62-214744	9/21/1987	Hitachi Ltd.		English Abstract	

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.	
AN	D1	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)	
AN	D2	D.W. Davies and W.L. Price, edited by Tadahiro Uezono, "Network Security", Japan, Nikkei McGraw-Hill, December 5, 1958, First Edition, first copy, p. 102-108	
EXAMINER 		DATE CONSIDERED 6/8/00	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
 1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control No.	95/001,270
				Patent No.	7,188,180
				Issued Date	March 6, 2007
				First Named Inventor	Victor Larson
				Docket Number	077580-0090
Sheet	1	of	19		

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code? (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
AN	A1000	5,303,302	04/12/1994	Burrows	
	A1000	5,311,593	05/10/1994	Carmi	
	A1001	5,384,848	01/24/1995	Kikuchi	
	A1002	5,511,122	04/23/1996	Atkinson	
	A1003	5,629,984	05/13/1997	McManis	
	A1004	5,771,239	06/23/1998	Moroney, et al.	
	A1005	5,805,803	09/08/1998	Birrell et al.	
	A1006	5,822,434	10/13/1998	Caronni et al.	
	A1007	5,898,830	04/27/1999	Wesinger, Jr. et al.	
	A1008	5,950,195	09/07/1999	Stockwell et al.	
	A1009	60/134,547	05/17/1999	Victor Sheymov	
	A1010	60/151,563	08/31/1999	Bryan Whittles	
	A1011	6,119,171	09/12/2000	Alkhatib	
	A1012	6,937,597	08/30/2005	Rosenberg et al.	
	A1013	7,072,964	07/04/2006	Whittle et al.	
	A1014	09/399,753	09/22/1998	Graig Miller et al.	
	A1015	6,079,020	06/20/2000	Liu	
	A1016	6,173,399	01/09/2001	Gilbrech	
	A1017	6,223,287	04/24/2001	Douglas, et al.	
	A1018	6,226,748	05/01/2001	Bots et al.	
	A1019	6,226,751	05/01/2001	Arrow et al.	
	A1020	6,701,437	03/02/2004	Hoke et al.	
	A1021	6,055,574	04/25/2000	Smorodinsky et al.	
	A1022	6,246,670	06/12/2001	Karlsson, et al.	
	A1023	7,461,334	12/02/08	Lu, et al.	
	A1024	7,353,841	04/08/08	Kono, et al.	
	A1025	7,188,175	03/06/07	McKeeth, James A.	
	A1026	7,167,904	01/23/07	Devarajan, et al.	
	A1027	7,039,713	05/02/06	Van Gunter, et al.	
	A1028	6,757,740	06/29/04	Parekh, et al.	
	A1029	6,752,166	06/22/04	Lull, et al.	
	A1030	6,687,746	02/03/04	Shuster, et al.	
	A1031	6,338,082	01/08/02	Schneider, Eric	
A1032	6,333,272	12/25/01	McMillin, et al.		

EXAMINER 	DATE CONSIDERED 6/8/10
---	---------------------------

*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 <i>(Use as many sheets as necessary)</i>				Complete if Known		
				Control No.	95/001,270	
				Patent No.	7,188,180	
				Issued Date	March 6, 2007	
				First Named Inventor	Victor Larson	
				Docket Number	077580-0090	
Sheet	3	of	19			

FOREIGN PATENT DOCUMENTS							
EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes - Number - Kind Codes (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No
AM ↓	B1000	WO 001/17775	03-30-2000	Science Applications International Corporation			
	B1001	WO 00/70458	11-23-2000	Comsec Corporation			
	B1002	WO 01/016766	03-08-2001	Science Applications International Corporation			
EXAMINER <i>GC</i>				DATE CONSIDERED <i>6/18/10</i>			

if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
 1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control No.	95/001,270
				Patent No.	7,188,180
				Issued Date	March 6, 2007
				First Named Inventor	Victor Larson
				Docket Number	077580-0090
Sheet	4	of	19		

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

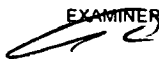
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
	C998	Microsoft Corporation's Fourth Amended Invalidation Contentions dated Jan. 5, 2009, VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation,
	C999	Appendix A of the Microsoft Corporation's Fourth Amended Invalidation Contentions dated Jan. 5, 2009.
	C1000	Concordance Table For the References Cited in Tables on pages 6-15, 71-80 and 116-124 of the Microsoft Corporation's Fourth Amended Invalidation Contentions dated Jan. 5, 2009.
	C1001	1. P. Mockapetris, "DNS Encoding of Network Names and Other Types," Network Working Group, RFC 1101 (April 1989) (RFC1101, DNS SRV)
	C1002	DNS-related correspondence dated September 7, 1993 to September 20, 1993. (Pre KX, KX Records)
	C1003	R. Atkinson, "An Internetwork Authentication Architecture," Naval Research Laboratory, Center for High Assurance Computing Systems (8/5/93). (Atkinson NRL, KX Records)
	C1004	Henning Schulzrinne, <i>Personal Mobility For Multimedia Services In The Internet</i> , Proceedings of the Interactive Distributed Multimedia Systems and Services European Workshop at 143 (1996). (Schulzrinne 96)
	C1005	Microsoft Corp., <i>Microsoft Virtual Private Networking: Using Point-to-Point Tunneling Protocol for Low-Cost, Secure, Remote Access Across the Internet</i> (1996) (printed from 1998 PDC DVD-ROM). (Point to Point, Microsoft Prior Art VPN Technology)
	C1006	"Safe Surfing: How to Build a Secure World Wide Web Connection," IBM Technical Support Organization, (March 1996). (Safe Surfing, WEBSITE ART)
	C1007	Goldschlag, et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK (May 1996). (Goldschlag II, Onion Routing)
	C1008	"IPSec Minutes From Montreal", IPSEC Working Group Meeting Notes, http://www.sandleman.ca/ipsec/1996/08/msg00018.html (June 1996). (IPSec Minutes, FreeSWAN)
	C1009	J. M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California, July 1996. (Galvin, DNSSEC)
C1010	J. Gilmore, et al. "Re: Key Management, anyone? (DNS Keying)," IPsec Working Group Mailing List Archives (8/96). (Gilmore DNS, FreeSWAN)	
C1011	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, FreeSWAN)	
C1012	Arnt Gulbrandsen & Paul Vixie, <i>A DNS RR for specifying the location of services (DNS SRV)</i> , IETF RFC 2052 (October 1996). (RFC 2052, DNS SRV)	

EXAMINER 	DATE CONSIDERED
--------------	---------------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
 1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control No.	95/001,270
				Patent No.	7,188,180
				Issued Date	March 6, 2007
				First Named Inventor	Victor Larson
				Docket Number	077580-0090
Sheet	5	of	19		

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.
AN	C1013	Freier, et al. "The SSL Protocol Version 3.0," Transport Layer Security Working Group (November 18, 1996). (SSL, UNDERLYING SECURITY TECHNOLOGY)
	C1014	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/02/1996). (RFC 2543 Internet Draft 1)
	C1015	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)
	C1016	Kenneth F. Alden & Edward P. Wobber, <i>The AltaVista Tunnel: Using the Internet to Extend Corporate Networks</i> , Digital Technical Journal (1997) (Alden, AltaVista)
	C1017	Automotive Industry Action Group, "ANX Release 1 Document Publication," AIAG (1997). (AIAG, ANX)
	C1018	Automotive Industry Action Group, "ANX Release 1 Draft Document Publication," AIAG Publications (1997). (AIAG Release, ANX)
	C1019	Aventail Corp., "AutoSOCKS v. 2.1 Datasheet," available at http://www.archive.org/web/19970212013409/www.aventail.com/prod/autosk2ds.html (1997). (AutoSOCKS, Aventail)
	C1020	Aventail Corp. "Aventail VPN Data Sheet," available at http://www.archive.org/web/19970212013043/www.aventail.com/prod/vpndata.html (1997). (Data Sheet, Aventail)
	C1021	Aventail Corp., "Directed VPN Vs. Tunnel," available at http://web.archive.org/web/19970620030312/www.aventail.com/educate/directvpn.html (1997). (Directed VPN, Aventail)
	C1022	Aventail Corp., "Managing Corporate Access to the Internet," Aventail AutoSOCKS White Paper available at http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/ipmwp.html (1997). (Corporate Access, Aventail)
	C1023	Aventail Corp., "Socks Version 5," Aventail Whitepaper, available at http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/sockswp.html (1997). (Socks, Aventail)
	C1024	Aventail Corp., "VPN Server V2.0 Administration Guide," (1997). (VPN, Aventail)
	C1025	Goldschlag, et al. "Privacy on the Internet," Naval Research Laboratory, Center for High Assurance Computer Systems (1997). (Goldschlag I, Onion Routing)
EXAMINER 		DATE CONSIDERED 6/8/10

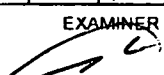
*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO			Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>			Control No.	95/001,270
			Patent No.	7,188,180
			Issued Date	March 6, 2007
			First Named Inventor	Victor Larson
			Docket Number	077580-0090
Sheet	6	of	19	

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

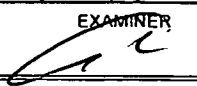
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
	C1026	Microsoft Corp., <i>Installing Configuring and Using PPTP with Microsoft Clients and Servers</i> (1997). (Using PPTP, Microsoft Prior Art VPN Technology)
	C1027	Microsoft Corp., <i>IP Security for Microsoft Windows NT Server 5.0</i> (1997) (printed from 1998 PDC DVD-ROM). (IP Security, Microsoft Prior Art VPN Technology)
	C1028	Microsoft Corp., <i>Microsoft Windows NT Active Directory: An Introduction to the Next Generation Directory Services</i> (1997) (printed from 1998 PDC DVD-ROM). (Directory, Microsoft Prior Art VPN Technology)
	C1029	Microsoft Corp., <i>Routing and Remote Access Service for Windows NT Server New Opportunities Today and Looking Ahead</i> (1997) (printed from 1998 PDC DVD-ROM). (Routing, Microsoft Prior Art VPN Technology)
	C1030	Microsoft Corp., <i>Understanding Point-to-Point Tunneling Protocol PPTP</i> (1997) (printed from 1998 PDC DVD-ROM). (Understanding PPTP, Microsoft Prior Art VPN Technology)
	C1031	J. Mark Smith et al., <i>Protecting a Private Network: The AltaVista Firewall</i> , Digital Technical Journal (1997). (Smith, AltaVista)
	C1032	Naganand Doraswamy <i>Implementation of Virtual Private Networks (VPNs) with IP Security</i> , <draft-ietf-ipsec-vpn-00.txt> (March 12, 1997). (Doraswamy)
	C1033	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, <i>Internet Draft, (03/27/1997). (RFC 2543 Internet Draft 2)</i>
	C1034	Aventail Corp., "Aventail and Cybersafe to Provide Secure Authentication For Internet and Intranet Communication," Press Release, April 3, 1997. (Secure Authentication, Aventail)
	C1035	D. Wagner, et al. "Analysis of the SSL 3.0 Protocol," (April 15, 1997). (Analysis, UNDERLYING SECURITY TECHNOLOGIES)
	C1036	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 Defintion, ANX)
	C1037	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)
	C1038	Aventail Corp., "Aventail Announces the First VPN Solution to Assure Interoperability Across Emerging Security Protocols," June 2, 1997. (First VPN, Aventail)
	C1039	Syverson, et al. "Private Web Browsing," Naval Research Laboratory, Center for High 8 Assurance Computer Systems (June 2, 1997). (Syverson, Onion Routing)
C1040	Bellcore, "Metrics, Criteria, and Measurement Technique Requirements for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (June 16, 1997). (AIAG Requirements, ANX)	
EXAMINER		DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control No.	95/001,270
				Patent No.	7,188,180
				Issued Date	March 6, 2007
				First Named Inventor	Victor Larson
				Docket Number	077580-0090
Sheet	7	of	19		
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.			
AN	C1041	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/31/1997). (RFC 2543 Internet Draft 3)			
	C1042	R. Atkinson, "Key Exchange Delegation Record for the DNS," Network Working Group, RFC 2230 (November 1997). (RFC 2230, KX Records)			
	C1043	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/11/1997). (RFC 2543 Internet Draft 4)			
	C1044	1998 Microsoft Professional Developers Conference DVD ("1998 PDC DVD-ROM") (including screenshots captured therefrom and produced as MSFTVX 00018827-00018832). (Conference, Microsoft Prior Art VPN Technology)			
	C1045	Microsoft Corp., <i>Virtual Private Networking An Overview</i> (1998) (printed from 1998 PDC DVD-ROM) (Overview, Microsoft Prior Art VPN Technology)			
	C1046	Microsoft Corp., <i>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</i> (1998) (available at http://www.microsoft.com/presspass/features/1998/10-19nt5.mspxptrue). (NT Beta, Microsoft Prior Art VPN Technology)			
	C1047	"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)			
	C1048	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)			
	C1049	R. G. Moskowitz, "Network Address Translation Issues with IPsec," Internet Draft, Internet Engineering Task Force, February 6, 1998. (Moskowitz)			
	C1050	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)			
	C1051	C. Huitema, et al. "Simple Gateway Control Protocol," Version 1.0 (May 5, 1998). (SGCP)			
	C1052	DISA "Secret Internet Protocol Router Network," SIPRNET Program Management Office (D3113) DISN Networks, DISN Transmission Services (May 8, 1998). (DISA, SIPRNET)			
	C1053	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (05/14/1998). (RFC 2543 Internet Draft 5)			
	C1054	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (06/17/1998). (RFC 2543 Internet Draft 6)			
	C1055	D. McDonald, et al. "PF_KEY Key Management API, Version 2," Network Working Group, RFC 2367 (July 1998). (RFC 2367)			
EXAMINER			DATE CONSIDERED		
			6/8/10		

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control No.	95/001,270
				Patent No.	7,188,180
				Issued Date	March 6, 2007
				First Named Inventor	Victor Larson
				Docket Number	077580-0090
Sheet	8	of	19		
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.			
AN	C1056	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/16/1998). (RFC 2543 Internet Draft 7)			
	C1057	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (08/07/1998). (RFC 2543 Internet Draft 8)			
	C1058	Microsoft Corp., <i>Company Focuses on Quality and Customer Feedback</i> (August 18, 1998). (Focus, Microsoft Prior Art VPN Technology)			
	C1059	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (09/18/1998). (RFC 2543 Internet Draft 9)			
	C1060	Atkinson, et al. "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998). (RFC 2401, UNDERLYING SECURITY TECHNOLOGIES)			
	C1061	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/12/1998). (RFC 2543 Internet Draft 10) 9			
	C1062	Donald Eastlake, <i>Domain Name System Security Extensions</i> , IETF DNS Security Working Group (December 1998). (DNSSEC-7)			
	C1063	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/15/1998). (RFC 2543 Internet Draft 11)			
	C1064	Aventail Corp., "Aventail Connect 3.1/2.6 Administrator's Guide," (1999). (Aventail Administrator 3.1, Aventail)			
	C1065	Aventail Corp., "Aventail Connect 3.1/2.6 User's Guide," (1999). (Aventail User 3.1, Aventail)			
	C1066	Aventail Corp., "Aventail ExtraWeb Server v3.2 Administrator's Guide," (1999). (Aventail ExtraWeb 3.2, Aventail)			
	C1067	Kaufman et al, "Implementing IPsec," (Copyright 1999). (Implementing IPSEC, VPN REFERENCES)			
	C1068	Network Solutions, Inc. "Enabling SSL," NSI Registry (1999). (Enabling SSL, UNDERLYING SECURITY TECHNOLOGIES)			
	C1069	Check Point Software Technologies Ltd. (1999) (Check Point, Checkpoint FW)			
	C1070	Arnt Gulbrandsen & Paul Vixie, <i>A DNS RR for specifying the location of services (DNS SRV)</i> , <draft-ietf-dnsind-frc2052bis-02.txt> (January 1999). (Gulbrandsen 99, DNS SRV)			
	C1071	C. Scott, et al. <i>Virtual Private Networks</i> , O'Reilly and Associates, Inc., 2nd ed. (Jan. 1999). (Scott VPNs)			
	C1072	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (01/15/1999). (RFC 2543 Internet Draft 12)			
	C1073	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)			
EXAMINER				DATE CONSIDERED	
				6/8/10	

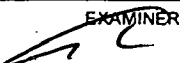

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

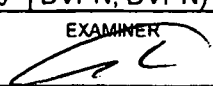
Subst. for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control No.	95/001,270
				Patent No.	7,188,180
				Issued Date	March 6, 2007
				First Named Inventor	Victor Larson
				Docket Number	077580-0090
Sheet	9	of	19		

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.
AN	C1074	H. Schulzrinne, "Internet Telephony: architecture and protocols – an IETF perspective," <i>Computer Networks</i> , Vol. 31, No. 3 (February 1999). (Telephony, Schulzrinne)
	C1075	M. Handley, et al. "SIP: Session Initiation Protocol," Network Working Group, RFC 2543 and Internet Drafts (12/96-3/99). (Handley, RFC 2543)
	C1076	FreeSWAN Project, <i>Linux FreeSWAN Compatibility Guide</i> (March 4, 1999). (FreeSWAN Compatibility Guide, FreeSWAN)
	C1077	Telcordia Technologies, "ANX Release 1 Document Corrections," AIAG (May 11, 1999). (Telcordia, ANX)
	C1078	Ken Hornstein & Jeffrey Altman, <i>Distributing Kerberos KDC and Realm Information with DNS <draft-eitf-cat-krb-dns-locate-oo.txt></i> (June 21, 1999). (Hornstein, DNS SRV)
	C1079	Bhattacharya et al. "An LDAP Schema for Configuration and Administration of IPSec Based Virtual Private Networks (VPNs)", IETF Internet Draft (October 1999). (Bhattacharya LDAP VPN)
	C1080	B. Patel, et al. "DHCP Configuration of IPSEC Tunnel Mode," IPSEC Working Group, Internet Draft 02 (10/15/1999). (Patel)
	C1081	Goncalves, et al. <i>Check Point FireWall -1 Administration Guide</i> , McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW)
	C1082	"Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources," FirstVPN, (Jan 2000). (FirstVPN Microsoft)
	C1083	Gulbrandsen, Vixie, & Esibov, <i>A DNS RR for specifying the location of services (DNS SRV)</i> , IETF RFC 2782 (February 2000). (RFC 2782, DNS SRV)
	C1084	MITRE Organization, "Technical Description," Collaborative Operations in Joint Expeditionary Force Experiment (JEFX) 99 (February 2000). (MITRE, SIPRNET)
	C1085	H. Schulzrinne, et al. "Application-Layer Mobility Using SIP," <i>Mobile Computing and Communications Review</i> , Vol. 4, No. 3. pp. 47-57 (July 2000). (Application, SIP)
	C1086	Kindred et al, "Dynamic VPN Communities: Implementation and Experience," DARPA Information Survivability Conference and Exposition II (June 2001). (DARPA, VPN SYSTEMS)
	C1087	ANX 101: Basic ANX Service Outline. (Outline, ANX)
	C1088	ANX 201: Advanced ANX Service. (Advanced, ANX)
	C1089	Appendix A: Certificate Profile for ANX IPsec Certificates. (Appendix, ANX)
↓	C1090	Assured Digital Products. (Assured Digital)

EXAMINER 	DATE CONSIDERED 
---	--

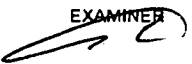
*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
 1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Control No.	95/001,270
				Patent No.	7,188,180
				Issued Date	March 6, 2007
				First Named Inventor	Victor Larson
				Docket Number	077580-0090
Sheet	10	of	19		
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.			
AN	C1091	Aventail Corp., "Aventail AutoSOCKS the Client Key to Network Security," Aventail Corporation White Paper. (Network Security, Aventail)			
	C1092	Cindy Moran, "DISN Data Networks: Secret Internet Protocol Router Network (SIPRNet)." (Moran, SIPRNET)			
	C1093	Data Fellows F-Secure VPN+ (F-Secure VPN+)			
	C1094	"Interim Operational Systems Doctrine for the Remote Access Security Program (RASP) Secret Dial-In Solution. (RASP, SIPRNET)			
	C1095	Onion Routing, "Investigation of Route Selection Algorithms," available at http://www.onion-router.net/Archives/Route/index.html . (Route Selection, Onion Routing)			
	C1096	Secure Computing, "Bullet-Proofing an Army Net," Washington Technology. (Secure, SIPRNET)			
	C1097	SPARTA "Dynamic Virtual Private Network." (Sparta, VPN SYSTEMS)			
	C1098	Standard Operation Procedure for Using the 1910 Secure Modems. (Standard, SIPRNET)			
	C1099	Publically available emails relating to FreeSWAN (MSFTVX00018833-MSFTVX00019206). (FreeS/WAN emails, FreeS/WAN)			
	C1100	Kaufman et al., "Implementing IPsec," (Copyright 1999) (Implementing IPsec)			
	C1101	Network Associates <i>Gauntlet Firewall For Unix User's Guide Version 5.0</i> (1999). (Gauntlet User's Guide - Unix, Firewall Products)			
	C1102	Network Associates <i>Gauntlet Firewall For Windows NT Getting Started Guide Version 5.0</i> (1999) (Gauntlet Getting Started Guide - NT, Firewall Products)			
	C1103	Network Associates <i>Gauntlet Firewall For Unix Getting Started Guide Version 5.0</i> (1999) (Gauntlet Unix Getting Started Guide, Firewall Products)			
	C1104	Network Associates <i>Release Notes Gauntlet Firewall for Unix 5.0</i> (March 19, 1999) (Gauntlet Unix Release Notes, Firewall Products)			
	C1105	Network Associates <i>Gauntlet Firewall For Windows NT Administrator's Guide Version 5.0</i> (1999) (Gauntlet NT Administrator's Guide, Firewall Products)			
	C1106	Trusted Information Systems, Inc. <i>Gauntlet Internet Firewall Firewall-to-Firewall Encryption Guide Version 3.1</i> (1996) (Gauntlet Firewall-to-Firewall, Firewall Products)			
	C1107	Network Associates <i>Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0</i> (1999) (Gauntlet NT GVPN, GVPN)			
	C1108	Network Associates <i>Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0</i> (1999) (Gauntlet Unix GVPN, GVPN)			
	C1109	Dan Sterne <i>Dynamic Virtual Private Networks</i> (May 23, 2000) (Sterne DVPN, DVPN)			
	C1110	Darrell Kindred <i>Dynamic Virtual Private Networks (DVPN)</i> (December 21, 1999) (Kindred DVPN, DVPN)			
EXAMINER				DATE CONSIDERED	
				6/18/10	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
 1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO		Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>		Control No.	95/001,270
		Patent No.	7,188,180
		Issued Date	March 6, 2007
		First Named Inventor	Victor Larson
		Docket Number	077580-0090
Sheet	11	of	19

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.
AN	C1111	Dan Sterne <i>et. al.</i> <i>TIS Dynamic Security Perimeter Research Project Demonstration</i> (March 9, 1998) (Dynamic Security Perimeter, DVPN)
	C1112	Darrell Kindred <i>Dynamic Virtual Private Networks Capability Description</i> (January 5, 2000) (Kindred DVPN Capability, DVPN) 11
	C1113	October 7, and 28 1997 email from Domenic J. Turchi Jr. (SPARTA00001712-1714, 1808-1811) (Turchi DVPN email, DVPN)
	C1114	James Just & Dan Sterne <i>Security Quickstart Task Update</i> (February 5, 1997) (Security Quickstart, DVPN)
	C1115	Virtual Private Network Demonstration dated March 21, 1998 (SPARTA00001844-54) (DVPN Demonstration, DVPN)
	C1116	GTE Internetworking & BBN Technologies <i>DARPA Information Assurance Program Integrated Feasibility Demonstration (IFD) 1.1 Plan</i> (March 10, 1998) (IFD 1.1, DVPN)
	C1117	Microsoft Corp. Windows NT Server Product Documentation: Administration Guide – Connection Point Services, <i>available at</i> 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.)
	C1118	Microsoft Corp. Windows NT Server Product Documentation: Administration Kit Guide – Connection Manager, <i>available at</i> http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cmak.msp (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.)
	C1119	Microsoft Corp. Autodial Heuristics, <i>available at</i> 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.)
	C1120	Microsoft Corp., Cariplo: Distributed Component Object Model, (1996) <i>available at</i> http://msdn2.microsoft.com/en-us/library/ms809332(printer).aspx (Cariplo I)
	C1121	Marc Levy, COM Internet Services (Apr. 23, 1999), <i>available at</i> http://msdn2.microsoft.com/en-us/library/ms809302(printer).aspx (Levy)
✓	C1122	Markus Horstmann and Mary Kirtland, DCOM Architecture (July 23, 1997), <i>available at</i> http://msdn2.microsoft.com/en-us/library/ms809311(printer).aspx (Horstmann)
EXAMINER 		DATE CONSIDERED <i>6/8/10</i>

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
 1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control No.	95/001,270
				Patent No.	7,188,180
				Issued Date	March 6, 2007
				First Named Inventor	Victor Larson
				Docket Number	077580-0090
Sheet	12	of	19		

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.
AN	C1123	Microsoft Corp., DCOM: A Business Overview (Apr. 1997), available at http://msdn2.microsoft.com/en-us/library/ms809320(printer).aspx (DCOM Business Overview I)
	C1124	Microsoft Corp., DCOM Technical Overview (Nov. 1996), available at http://msdn2.microsoft.com/en-us/library/ms809340(printer).aspx (DCOM Technical Overview I)
	C1125	Microsoft Corp., DCOM Architecture White Paper (1998) available in PDC DVD-ROM (DCOM Architecture)
	C1126	Microsoft Corp, DCOM – The Distributed Component Object Model, A Business Overview White Paper (Microsoft 1997) available in PDC DVD-ROM (DCOM Business Overview II)
	C1127	Microsoft Corp., DCOM—Cariplo Home Banking Over The Internet White Paper (Microsoft 1996) available in PDC DVD-ROM (Cariplo II)
	C1128	Microsoft Corp., DCOM Solutions in Action White Paper (Microsoft 1996) available in PDC DVD-ROM (DCOM Solutions in Action)
	C1129	Microsoft Corp., DCOM Technical Overview White Paper (Microsoft 1996) available in PDC DVD-ROM (DCOM Technical Overview II)
	C1130	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)
	C1131	126. Aaron Skonnard, <i>Essential Winlnet</i> 313-423 (Addison Wesley Longman 1998) (Essential Winlnet)
	C1132	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)
	C1133	Microsoft Corp., Internet Connection Services for MS RAS, Standard Edition, http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstart.msp (Internet Connection Services I)
	C1134	Microsoft Corp., Internet Connection Services for RAS, Commercial Edition, available at http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstrtc.msp (Internet Connection Services II)
	C1135	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.msp (IE5 Corporate Development)
	C1136	Mark Minasi, <i>Mastering Windows NT Server 4</i> 1359-1442 (6th ed., January 15, 1999)(Mastering Windows NT Server)
✓	C1137	<i>Hands On, Self-Paced Training for Supporting Version 4.0</i> 371-473 (Microsoft Press 1998) (Hands On)

EXAMINER 	DATE CONSIDERED 6/8/00
---	---------------------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
 1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control No.	95/001,270
				Patent No.	7,188,180
				Issued Date	March 6, 2007
				First Named Inventor	Victor Larson
				Docket Number	077580-0090
Sheet	13	of	19		

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.
AN	C1138	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)
	C1139	Kenneth Gregg, et al., <i>Microsoft Windows NT Server Administrator's Bible</i> 173-206, 883-911, 974-1076 (IDG Books Worldwide 1999) (Gregg)
	C1140	Microsoft Corp., Remote Access (Windows), available at http://msdn2.microsoft.com/en-us/library/bb545687(VS.85,printer).aspx (Remote Access)
	C1141	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.)
	C1142	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.)
	C1143	Anthony Northrup, <i>NT Network Plumbing: Routers, Proxies, and Web Services</i> 299-399 (IDG Books Worldwide 1998) (Network Plumbing)
	C1144	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/rrasch01.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
	C1145	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.)
	C1146	F-Secure, <i>F-Secure Evaluation Kit</i> (May 1999) (FSECURE 00000003) (Evaluation Kit 3)
	C1147	F-Secure, <i>F-Secure NameSurfer</i> (May 1999) (from FSECURE 00000003) (NameSurfer 3)
✓	C1148	F-Secure, <i>F-Secure VPN Administrator's Guide</i> (May 1999) (from FSECURE 00000003) (F-Secure VPN 3)

EXAMINER 	DATE CONSIDERED 6/8/00
---	---------------------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
 1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control No.	95/001,270
				Patent No.	7,188,180
				Issued Date	March 6, 2007
				First Named Inventor	Victor Larson
				Docket Number	077580-0090
Sheet	14	of	19		

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.
AN	C1149	F-Secure, <i>F-Secure SSH User's & Administrator's Guide</i> (May 1999) (from FSECURE 00000003) (SSH Guide 3)
	C1150	F-Secure, <i>F-Secure SSH 2.0 for Windows NT and 95</i> (May 1999) (from FSECURE 00000003) (SSH 2.0 Guide 3)
	C1151	F-Secure, <i>F-Secure VPN+ Administrator's Guide</i> (May 1999) (from FSECURE 00000003) (VPN+ Guide 3)
	C1152	F-Secure, <i>F-Secure VPN+ 4.1</i> (1999) (from FSECURE 00000006) (VPN+ 4.1 Guide 6)
	C1153	F-Secure, <i>F-Secure SSH</i> (1996) (from FSECURE 00000006) (F-Secure SSH 6)
	C1154	F-Secure, <i>F-Secure SSH 2.0 for Windows NT and 95</i> (1998) (from FSECURE 00000006) (F-Secure SSH 2.0 Guide 6)
	C1155	F-Secure, <i>F-Secure Evaluation Kit</i> (Sept. 1998) (FSECURE 00000009) (Evaluation Kit 9)
	C1156	F-Secure, <i>F-Secure SSH User's & Administrator's Guide</i> (Sept. 1998) (from FSECURE 00000009) (SSH Guide 9)
	C1157	F-Secure, <i>F-Secure SSH 2.0 for Windows NT and 95</i> (Sept. 1998) (from FSECURE 00000009) (F-Secure SSH 2.0 Guide 9)
	C1158	F-Secure, <i>F-Secure VPN+</i> (Sept. 1998) (from FSECURE 00000009) (VPN+ Guide 9)
	C1159	F-Secure, <i>F-Secure Management Tools, Administrator's Guide</i> (1999) (from FSECURE 00000003) (F-Secure Management Tools)
	C1160	F-Secure, <i>F-Secure Desktop, User's Guide</i> (1997) (from FSECURE 00000009) (FSecure Desktop User's Guide)
	C1161	SafeNet, Inc., <i>VPN Policy Manager</i> (January 2000) (VPN Policy Manager)
	C1162	F-Secure, <i>F-Secure VPN+ for Windows NT 4.0</i> (1998) (from FSECURE 00000009) (FSecure VPN+)
	C1163	IRE, Inc., <i>SafeNet/Soft-PK Version 4</i> (March 28, 2000) (Soft-PK Version 4)
	C1164	IRE/SafeNet Inc., <i>VPN Technologies Overview</i> (March 28, 2000) (Safenet VPN Overview)
	C1165	IRE, Inc., <i>SafeNet / Security Center Technical Reference Addendum</i> (June 22, 1999) (Safenet Addendum)
	C1166	IRE, Inc., <i>System Description for VPN Policy Manager and SafeNet/SoftPK</i> (March 30, 2000) (VPN Policy Manager System Description)
	C1167	IRE, Inc., <i>About SafeNet / VPN Policy Manager</i> (1999) (About Safenet VPN Policy Manager)
	C1168	IRE, Inc., <i>SafeNet/VPN Policy Manager Quick Start Guide Version 1</i> (1999) (SafeNet VPN Policy Manager)
EXAMINER 		DATE CONSIDERED 6/21/00

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
 1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO			Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>			Control No.	95/001,270
			Patent No.	7,188,180
			Issued Date	March 6, 2007
			First Named Inventor	Victor Larson
			Docket Number	077580-0090
Sheet	15	of	19	

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.
AN	C1169	Trusted Information Systems, Inc., <i>Gauntlet Internet Firewall, Firewall Product Functional Summary</i> (July 22, 1996) (Gauntlet Functional Summary)
	C1170	Trusted Information Systems, Inc., <i>Running the Gauntlet Internet Firewall, An Administrator's Guide to Gauntlet Version 3.0</i> (May 31, 1995) (Running the Gauntlet Internet Firewall)
	C1171	Ted Harwood, <i>Windows NT Terminal Server and Citrix Metaframe</i> (New Riders 1999) (Windows NT Harwood) 79
	C1172	Todd W. Matehrs and Shawn P. Genoway, <i>Windows NT Thing Client Solutions: Implemetning Terminal Server and Citrix MetaFrame</i> (Macmillan Technial Publishing 1999) (Windows NT Mathers)
	C1173	Bernard Aboba et al., <i>Securing L2TP using IPSEC</i> (February 2, 1999)
	C1174	156. <i>Finding Your Way Through the VPN Maze</i> (1999) ("PGP")
	C1175	Linux FreeSWAN Overview (1999) (Linux FreeSWAN) Overview)
	C1176	TimeStep, <i>The Business Case for Secure VPNs</i> (1998) ("TimeStep")
	C1177	WatchGuard Technologies, Inc., <i>WatchGuard Firebox System Powerpoint</i> (2000)
	C1178	WatchGuard Technologies, Inc., <i>MSS Firewall Specifications</i> (1999)
	C1179	WatchGuard Technologies, Inc., <i>Request for Information, Security Services</i> (2000)
	C1180	WatchGuard Technologies, Inc., <i>Protecting the Internet Distributed Enterprise, White Paper</i> (February 2000)
	C1181	WatchGuard Technologies, Inc., <i>WatchGuard LiveSecurity for MSS Powerpoint</i> (Feb. 14 2000)
	C1182	WatchGuard Technologies, Inc., <i>MSS Version 2.5, Add-On for WatchGuard SOHO Releaset Notes</i> (July 21, 2000)
	C1183	Air Force Research Laboratory, <i>Statement of Work for Information Assurance System Architecture and Integration, PR No. N-8-6106 (Contract No. F30602-98-C-0012)</i> (January 29, 1998)
	C1184	GTE Internetworking & BBN Technologies <i>DARPA Information Assurance Program Integrated Feasibility Demonstration (IFD) 1.2 Report, Rev. 1.0</i> (September 21, 1998)
✓	C1185	BBN Information Assurance Contract, <i>TIS Labs Monthly Status Report</i> (March 16-April 30, 1998)

EXAMINER 	DATE CONSIDERED 6/8/10
---	---------------------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
 1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Control No.	95/001,270
				Patent No.	7,188,180
				Issued Date	March 6, 2007
				First Named Inventor	Victor Larson
				Docket Number	077580-0090
Sheet	16	of	19		

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.
AN	C1186	DARPA, <i>Dynamic Virtual Private Network (VPN) Powerpoint</i>
	C1187	GTE Internetworking, <i>Contractor's Program Progress Report</i> (March 16-April 30, 1998)
	C1188	Darrell Kindred, <i>Dynamic Virtual Private Networks (DVPN) Countermeasure Characterization</i> (January 30, 2001)
	C1189	<i>Virtual Private Networking Countermeasure Characterization</i> (March 30, 2000)
	C1190	<i>Virtual Private Network Demonstration</i> (March 21, 1998)
	C1191	Information Assurance/NAI Labs, <i>Dynamic Virtual Private Networks (VPNs) and Integrated Security Management</i> (2000)
	C1192	Information Assurance/NAI Labs, <i>Create/Add DVPN Enclave</i> (2000)
	C1193	NAI Labs, <i>IFE 3.1 Integration Demo</i> (2000)
	C1194	Information Assurance, <i>Science Fair Agenda</i> (2000)
	C1195	Darrell Kindred et al., <i>Proposed Threads for IFE 3.1</i> (January 13, 2000)
	C1196	<i>IFE 3.1 Technology Dependencies</i> (2000)
	C1197	<i>IFE 3.1 Topology</i> (February 9, 2000)
	C1198	Information Assurance, <i>Information Assurance Integration: IFE 3.1, Hypothesis & Thread Development</i> (January 10-11, 2000)
	C1199	Information Assurance/NAI Labs, <i>Dynamic Virtual Private Networks Presentation</i> (2000)
	C1200	Information Assurance/NAI Labs, <i>Dynamic Virtual Private Networks Presentation v.2</i> (2000)
	C1201	Information Assurance/NAI Labs, <i>Dynamic Virtual Private Networks Presentation v.3</i> (2000)
C1202	T. Braun et al., <i>Virtual Private Network Architecture, Charging and Accounting Technology for the Internet</i> (August 1, 1999) (VPNA)	
C1203	Network Associates Products - <i>PGP Total Network Security Suite, Dynamic Virtual Private Networks</i> (1999)	
C1204	Microsoft Corporation, <i>Microsoft Proxy Server 2.0</i> (1997) (Proxy Server 2.0, Microsoft Prior Art VPN Technology)	
C1205	David Johnson et. al., <i>A Guide To Microsoft Proxy Server 2.0</i> (1999) (Johnson, Microsoft Prior Art VPN Technology)	
C1206	Microsoft Corporation, <i>Setting Server Parameters</i> (1997 (copied from Proxy Server 2.0 CD labeled MSFTVX00157288) (Setting Server Parameters, Microsoft Prior Art VPN Technology)	

EXAMINER 	DATE CONSIDERED 6/18/10
---	----------------------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
 1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO			Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)			Control No.	95/001,270	
			Patent No.	7,188,180	
			Issued Date	March 6, 2007	
			First Named Inventor	Victor Larson	
			Docket Number	077580-0090	
Sheet	17	of	19		

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.
AP	C1207	Kevin Schuler, <i>Microsoft Proxy Server 2</i> (1998) (Schuler, Microsoft Prior Art VPN Technology)
	C1208	Erik Rozell et. al., <i>MCSE Proxy Server 2 Study Guide</i> (1998) (Rozell, Microsoft Prior Art VPN Technology)
	C1209	M. Shane Stigler & Mark A Linsenbardt, <i>IIS 4 and Proxy Server 2</i> (1999) (Stigler, Microsoft Prior Art VPN Technology)
	C1210	David G. Schaer, <i>MCSE Test Success: Proxy Server 2</i> (1998) (Schaer, Microsoft Prior Art VPN Technology)
	C1211	John Savill, <i>The Windows NT and Windows 2000 Answer Book</i> (1999) (Savill, Microsoft Prior Art VPN Technology)
	C1212	Network Associates <i>Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0</i> (1999) (Gauntlet NT GVPN, GVPN)
	C1213	Network Associates <i>Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0</i> (1999) (Gauntlet Unix GVPN, GVPN)
	C1214	File History for U.S. Application Serial No. 09/653,201, Applicant(s): Whittle Bryan, et al., Filing Date 08/31/2000.
	C1215	<i>AutoSOCKS v2.1</i> , Datasheet, http://web.archive.org/web/19970212013409/www.aventail.com/prod/autoskds.html
	C1216	Ran Atkinson, <i>Use of DNS to Distribute Keys</i> , 7 Sept. 1993, http://ops.ietf.org/lists/namedroppers/namedroppers.199x/msg00945.html
	C1217	FirstVPN Enterprise Networks, Overview
	C1218	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
	C1219	The TLS Protocol Version 1.0; January 1999; page 65 of 71.
	C1220	Elizabeth D. Zwicky, et al., <i>Building Internet Firewalls</i> , 2nd Ed.
	C1221	Virtual Private Networks – Assured Digital Incorporated – ADI 4500; http://web.archive.org/web/19990224050035/www.assured-digital.com/products/prodvpn/adia4500.htm
	C1222	Accessware – The Third Wave in Network Security, Conclave from Internet Dynamics; http://web.archive.org/web/11980210013830/interdyn.com/Accessware.html
	C1223	Extended System Press Release, Sept. 2, 1997; <i>Extended VPN Uses The Internet to Create Virtual Private Networks</i> , www.extendedsystems.com
	C1224	Socks Version 5; Executive Summary; http://web.archive.org/web/199970620031945/www.aventail.com/educate/whitepaper/sockswp.html
✓	C1225	Internet Dynamics First to Ship Integrated Security Solutions for Enterprise Intranets and Extranets; Sept. 15, 1997; http://web.archive.org/web/19980210014150/interdyn.com

EXAMINER 	DATE CONSIDERED 6/8/10
---	---------------------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
 1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO		Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)		Control No.	95/001,270
		Patent No.	7,188,180
		Issued Date	March 6, 2007
		First Named Inventor	Victor Larson
		Docket Number	077580-0090
Sheet	18	of	19

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.
	C1226	Emails from various individuals to Linux IPsec re: DNS-LDAP Splicing
	C1227	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
	C1228	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
	C1229	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
	C1230	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
	C1231	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
	C1232	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
	C1233	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
	C1234	Derrell Piper, "The Internet IP Security Domain of Interpretation for ISAKMP," RFC 2407 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html
	C1235	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
	C1236	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
	C1237	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
	C1238	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
C1239	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")	
EXAMINER		DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
 1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Control No.	95/001,270
				Patent No.	7,188,180
				Issued Date	March 6, 2007
				First Named Inventor	Victor Larson
				Docket Number	077580-0090
Sheet	19	of	19		

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.
AL ↓	C1240	David Kosiur, "Building and Managing Virtual Private Networks" (1998)
	C1241	P. Mockapetris, "Domain Names - Implementation and Specification," Network Working Group, RFC 1035 (November 1987)
	C1242	Request for Inter Partes Reexamination of Patent No. 6,502,135, dated Nov. 25, 2009.
EXAMINER <i>AL</i>		DATE CONSIDERED <i>6/18/07</i>

*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.

BST99 1643905-1.077580.0090

EXHIBIT C

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION**

VirnetX Inc.

Plaintiff,

vs.

Cisco Systems, Inc., *et al.*,

Defendants.

§
§
§
§
§
§
§
§
§

Case No. 6:10-cv-417

JURY TRIAL DEMANDED

**DEFENDANT APPLE INC.’S ORIGINAL ANSWER, AFFIRMATIVE DEFENSES, AND
COUNTERCLAIMS TO PLAINTIFF’S ORIGINAL COMPLAINT**

Defendant Apple Inc. (“Apple”) files this Original Answer, Affirmative Defenses and Counterclaims to Plaintiff’s Original Complaint for Patent Infringement (the “Complaint”) filed by VirnetX Inc. (“VirnetX”).

I. ANSWER

THE PARTIES

1. - 2. Apple is without sufficient information or knowledge to either admit or deny the allegations in paragraphs 1 and 2 and therefore denies the same.

3. Apple admits that it is a California corporation organized and existing under the laws of California, with its principal place of business at One Infinite Loop, Cupertino, California 95014. Apple admits that it has conducted business in this district. Apple denies all other allegations contained in paragraph 3 of VirnetX’s complaint.

4. - 5. Apple is without sufficient information or knowledge to either admit or deny the allegations in paragraphs 4 and 5 and therefore denies the same.

JURISDICTION AND VENUE

6. Apple admits that VirnetX alleges a civil action for patent infringement under the laws of the United States, Title 35 United States Code §§ 101, *et seq.* Apple admits that this Court has subject matter jurisdiction over VirnetX's claims for patent infringement. Apple denies all other allegations contained in paragraph 6 of VirnetX's complaint.

7. To the extent the allegations in paragraph 7 relate to Apple, Apple admits that venue is proper in this Court, but Apple denies that this judicial district is the most convenient forum for this case. Apple denies all other allegations in this paragraph to the extent such allegations relate to Apple. To the extent the allegations in paragraph 7 relate to the other Defendants in this case, Apple is without sufficient information or knowledge to either admit or deny the allegations and therefore denies the same.

8. To the extent the allegations in paragraph 8 relate to Apple, Apple admits that this Court has personal jurisdiction over Apple. Apple admits that it has conducted business in the State of Texas. Apple admits that it has and does sell products and provide services to persons within the State of Texas and this District, but it denies that it has committed any acts of infringement within this District or the State of Texas, and specifically denies any wrongdoing, infringement, inducement of infringement, or contribution to infringement. Apple denies all other allegations in this paragraph to the extent such allegations relate to Apple. To the extent the allegations in paragraph 8 relate to the other Defendants in this case, Apple is without sufficient information or knowledge to either admit or deny the allegations and therefore denies the same.

ASSERTED PATENTS

9. Apple admits that, according to the face of the patent, United States Patent No. 6,502,135 (“the ‘135 patent”) is entitled “Agile Network Protocol for Secure Communications with Assured System Availability” and reflects an issue date of December 31, 2002. Apple admits that Edmund Colby Munger, Douglas Charles Schmidt, Robert Dunham Short, III, Victor Larson, and Michael Williamson are listed as inventors on the face of the patent. Apple admits that what appears to be a copy of the ‘135 patent is attached as Exhibit A to VirnetX’s Complaint. Apple denies all other allegations contained in paragraph 9 of VirnetX’s complaint.

10. Apple admits that, according to the face of the patent, United States Patent No. 6,839,759 (“the ‘759 patent”) is entitled “Method for Establishing Secure Communication Link Between Computers of Virtual Private Network Without User Entering Any Cryptographic Information” and reflects an issue date of January 4, 2005. Apple admits that Victor Larson, Robert Dunham Short, III, Edmund Colby Munger, and Michael Williamson are listed as inventors on the face of the patent. Apple admits that what appears to be a copy of the ‘759 patent is attached as Exhibit B to VirnetX’s Complaint. Apple denies all other allegations contained in paragraph 10 of VirnetX’s complaint.

11. Apple admits that, according to the face of the patent, United States Patent No. 7,188,180 (“the ‘180 patent”) is entitled “Method for Establishing Secure Communication Link Between Computers of Virtual Private Network” and reflects an issue date of March 6, 2007. Apple admits that Victor Larson, Robert Dunham Short, III, Edmund Colby Munger, and Michael Williamson are listed as inventors on the face of the patent. Apple admits that what appears to be a copy of the ‘180 patent is attached as Exhibit C to VirnetX’s Complaint. Apple denies all other allegations contained in paragraph 11 of VirnetX’s complaint.

12. Apple admits that, according to the face of the patent, United States Patent No. 7,418,504 (“the ‘504 patent”) is entitled “Agile Network Protocol for Secure Communications Using Secure Domain Names” and reflects an issue date of August 26, 2008. Apple admits that Victor Larson, Robert Dunham Short, III, Edmund Colby Munger, and Michael Williamson are listed as inventors on the face of the patent. Apple admits that what appears to be a copy of the ‘504 patent is attached as Exhibit D to VirnetX’s Complaint. Apple denies all other allegations contained in paragraph 12 of VirnetX’s complaint.

13. Apple admits that, according to the face of the patent, United States Patent No. 7,490,151 (“the ‘151 patent”) is entitled “Establishment of a Secure Communication Link Based on a Domain Name Service (DNS) Request” and reflects an issue date of February 10, 2009. Apple admits that Edmund Colby Munger, Robert Dunham Short, III, Victor Larson, and Michael Williamson are listed as inventors on the face of the patent. Apple admits that what appears to be a copy of the ‘151 patent is attached as Exhibit E to VirnetX’s Complaint. Apple denies all other allegations contained in paragraph 13 of VirnetX’s complaint.

COUNT ONE

ALLEGED PATENT INFRINGEMENT BY AASTRA

14. Apple incorporates by reference paragraphs 1-13 above as if fully set forth herein. Apple is without sufficient information or knowledge to either admit or deny the allegations in paragraph 14 regarding Aastra and the ‘135 patent and therefore denies the same.

15. – 22. Apple is without sufficient information or knowledge to either admit or deny the allegations in paragraphs 15-22 and therefore denies the same.

COUNT TWO

ALLEGED PATENT INFRINGEMENT BY APPLE

23. Apple incorporates by reference paragraphs 1-22 above as if fully set forth herein.

Apple denies that it has infringed or continues to infringe the '135 and '151 patents.

24. Denied.

25. Denied.

26. Apple admits that it provides or has provided the iPhone, iPhone 3G, iPhone 3GS, iPhone 4, iPod Touch, and iPad to others in the United States. Apple denies that these or any other Apple products infringe any asserted claims of the '135 patent. Apple further denies all other allegations contained in paragraph 26 of VirnetX's Complaint.

27. Denied.

28. Denied.

29. Apple admits that it makes, uses, sells, offers for sale, imports, exports, supplies, and/or distributes within and from the United States the iPhone, iPhone 3G, iPhone 3GS, iPhone 4, iPod Touch, and iPad, but it denies that these or any other Apple products infringe any asserted claims of the '151 patent. Apple further denies all other allegations contained in paragraph 29 of VirnetX's Complaint.

30. Apple admits that it makes, uses, sells, offers for sale, imports, exports, supplies, and/or distributes within and from the United States the iPhone, iPhone 3G, iPhone 3GS, iPhone 4, iPod Touch, and iPad, but it denies that these or any other Apple products infringe any asserted claims of the '151 patent. It is not clear what is referenced by "Apple's servers, master discs, and other media that store, cache, or distribute iPhone OS." As such, Apple denies the same. Apple further denies all other allegations contained in paragraph 30 of VirnetX's Complaint.

31. Apple admits that it provides or has provided the iPhone, iPhone 3G, iPhone 3GS, iPhone 4, iPod Touch, and iPad to others in the United States. Apple denies that these or any other Apple products infringe any asserted claims of the '151 patent. It is not clear what is referenced by "Apple's servers, master discs, and other media that store, cache, or distribute iPhone OS." As such, Apple denies the same. Apple further denies all other allegations contained in paragraph 31 of VirnetX's Complaint.

32. Denied.

33. Denied.

34. Denied.

35. Denied.

36. Apple admits that it received notice of infringement after the filing of this lawsuit but denies that any Apple products infringe the '135 or '151 patents. Apple further denies all other allegations contained in paragraph 36 of VirnetX's Complaint.

COUNT THREE

ALLEGED PATENT INFRINGEMENT BY CISCO

37. Apple incorporates by reference paragraphs 1-36 above as if fully set forth herein. Apple is without sufficient information or knowledge to either admit or deny the allegations in paragraph 37 regarding Cisco and the '135, '759, '180, and '504 patents and therefore denies the same.

38. – 63. Apple is without sufficient information or knowledge to either admit or deny the allegations in paragraphs 38-63 and therefore denies the same.

COUNT THREE

ALLEGED PATENT INFRINGEMENT BY NEC

64. Apple incorporates by reference paragraphs 1-63 above as if fully set forth herein. Apple is without sufficient information or knowledge to either admit or deny the allegations in paragraph 64 regarding NEC and the '135 and '504 patents and therefore denies the same.

65. - 77. Apple is without sufficient information or knowledge to either admit or deny the allegations in paragraphs 65-77 and therefore denies the same.

DEMAND FOR JURY TRIAL

Apple also demands a trial by jury.

PRAYER FOR RELIEF

Apple opposes VirnetX's requested relief against Apple or any other relief VirnetX requests against Apple, including those specified in paragraphs 1-17 of this Section of VirnetX's Complaint.

DENIAL OF ANY REMAINING ALLEGATIONS

Except as specifically admitted herein, Apple denies any remaining allegations in VirnetX's Complaint that are directed at Apple.

II. AFFIRMATIVE DEFENSES

Apple asserts the following Affirmative Defenses.

FIRST AFFIRMATIVE DEFENSE
(No Infringement)

78. Apple does not infringe and has not infringed any valid and enforceable claim of the '135 and '151 patents.

SECOND AFFIRMATIVE DEFENSE
(Invalidity)

79. Claims of the '135 and '151 patents are invalid for failure to satisfy the conditions for patentability set forth in Title 35 of the United States Code, including without limitation §§ 101, 102, 103 and 112.

THIRD AFFIRMATIVE DEFENSE
(Failure to State a Claim)

80. VirnetX's claims for relief and each and every one of its allegations fail to state a claim upon which relief can be granted.

FOURTH AFFIRMATIVE DEFENSE
(Laches)

81. VirnetX's claims are barred in whole or in part by laches.

FIFTH AFFIRMATIVE DEFENSE
(Waiver)

82. VirnetX's claims are barred in whole or in part by waiver.

SIXTH AFFIRMATIVE DEFENSE
(Estoppel)

83. VirnetX's claims are barred in whole or in part by estoppel.

SEVENTH AFFIRMATIVE DEFENSE
(Notice, Damages, and Costs)

84. VirnetX's claims for damages, if any, against Apple are statutorily limited by 35 U.S.C. § 286 and/or § 287.

85. VirnetX is barred from recovering costs in connection with this action under 35 U.S.C. § 288.

EIGHT AFFIRMATIVE DEFENSE
(Lack of Standing)

86. VirnetX lacks standing to enforce one or more of the patents-in-suit, including because it does not have all substantial rights in the patents. Upon information and belief, Science Application International Corp. (“SAIC”) retains substantial rights in one or more of the patents-in-suit and is a necessary party to this litigation.

NINTH AFFIRMATIVE DEFENSE
(Sales to Government)

87. VirnetX’s claims are limited by 28 U.S.C. § 1498.

TENTH AFFIRMATIVE DEFENSE
(Unclean Hands and Inequitable Conduct)

88. As more fully outlined in Apple’s Count III, specifically paragraphs 9-34 in Apple’s Counterclaims, which are hereby incorporated by reference, the claims of the ‘135 and ‘151 patents are unenforceable due to inequitable conduct, infectious unenforceability, and/or unclean hands committed by the inventors, their counsel, SAIC, VirnetX, and/or others substantively involved in the prosecution of the ‘135 or ‘151 patents.

RESERVATION OF AFFIRMATIVE DEFENSES

89. Apple hereby reserves the right to supplement additional affirmative defenses as discovery proceeds in this case.

III. COUNTERCLAIMS

Apple asserts the following counterclaims against VirnetX.

PARTIES

1. Counterclaim plaintiff is a California Corporation with its principal place of business at One Infinite Loop, Cupertino, California 95014.

2. On information and belief based on Plaintiff's Complaint, Counterclaim Defendant VirnetX Inc. ("VirnetX") is a Delaware corporation, having a place of business located at 5615 Scotts Valley Drive, Suite 110, Scotts Valley, California.

JURISDICTION AND VENUE

3. These counterclaims arise under the patent laws of the United States as enacted under Title 35 of the United States Code and the provisions of the Federal Declaratory Judgment Act. The jurisdiction of this Court is proper under 28 U.S.C. §§ 1331, 1338, 2201 and 2202.

4. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391 and 1400.

COUNT I – DECLARATION OF NON-INFRINGEMENT

5. Based on VirnetX's filing of this action and Apple's Affirmative Defenses, an actual controversy has arisen and now exists between VirnetX and Apple as to whether Apple has infringed or is infringing one or more claims of U.S. Patent Numbers 6,502,135 ("the '135 patent") and 7,490,151 ("the '151 patent").

6. Pursuant to the Federal Declaratory Judgment Act, 28 U.S.C. § 2201 *et seq.*, Apple requests the declaration of the Court that Apple does not infringe and has not infringed any valid and enforceable claim of the '135 and '151 patents.

COUNT II – DECLARATION OF PATENT INVALIDITY

7. Based on VirnetX's filing of this action and Apple's Affirmative Defenses, an actual controversy has arisen and now exists between VirnetX and Apple as to the validity of the claims of the '135 and '151 patents.

8. Pursuant to the Federal Declaratory Judgment Act, 28 U.S.C. § 2201 *et seq.*, Apple requests the declaration of the Court that the '135 and '151 patents are invalid.

COUNT III – DECLARATION OF UNENFORCEABILITY

9. Based on VirnetX's filing of this action and Apple's Affirmative Defenses, an actual controversy has arisen and now exists between VirnetX and Apple as to the enforceability of the '135 and '151 patents.

10. The '135 patent, which issued on December 31, 2002, was filed with the United States Patent and Trademark Office ("Patent Office") on February 15, 2000 as U.S. Patent Application No. 09/504,783 ("the '783 application").

11. The '151 patent, which issued on February 10, 2009, was filed with the United States Patent and Trademark Office ("Patent Office") on September 30, 2002 as U.S. Patent Application No. 10/259,494 ("the '494 application").

12. On information and belief, the applications that matured into the '135 and '151 patents were assigned to Science Application International Corporation ("SAIC"). On information and belief, SAIC assigned to VirnetX certain rights in the '135 patent after issuance and certain rights in the application that matured into the '151 patent.

A. The '135 Patent

13. The '135 patent is unenforceable due to inequitable conduct. Based on a review of the file history and based on Apple's understanding of the allegations by VirnetX, one or more of the people substantively involved in the prosecution of the application leading to the '135 patent, including a reexamination, were aware of information material to the patentability of the claims of the '135 patent, but withheld that information from the Patent Office with the intent to deceive.

14. The withheld information includes U.S. Patent Application No. 09/399,753 ("the Miller Application"), which was pending during the prosecution of the '135 patent. The pendency of the Miller Application was information material to patentability of the '135 patent

based on Apple's understanding of the allegations by VirnetX. The withheld information also includes RFC 2401-Security Architecture for the Internet Protocol ("RFC 2401") and information concerning the publication date of the Aventail Administrator's Guide ("Aventail"), which are material to patentability based upon Apple's understanding of the allegations by VirnetX. This withholding of information material to patentability with the intent to deceive the Patent Office constitutes inequitable conduct.

15. The Miller Application, RFC 2401, and the Aventail reference are not cumulative to the prior art made of record during prosecution of the '135 patent. On information and belief, there is a substantial likelihood that a reasonable examiner would have considered this art in determining whether to allow the '135 patent to issue.

16. During the prosecution of the application leading to the '135 patent, one or more of the people substantively involved in its prosecution (including Ross Dannenburg) were aware of the Miller Application. Mr. Dannenburg was involved in the prosecution of the Miller Application at least as early as June 14, 2002, when he signed an Amendment / Response in the prosecution history of the Miller Application. Mr. Dannenburg was involved in the prosecution of the '135 patent at least as early as January 28, 2002, when he signed a Transmittal Form for an Amendment / Response in the prosecution file history of the '135 patent. Therefore, Mr. Dannenburg was involved in the prosecution of the Miller Application while he was prosecuting the '135 patent. Based on Apple's understanding of the allegations by VirnetX, the pendency of the Miller Application is information material to patentability. Nonetheless, those substantively involved in the prosecution of the application intentionally failed to disclose this material information to the Patent Office at any time during the prosecution of the '135 patent with intent to deceive. Moreover, the materiality of the Miller Application leads to an inference of intent to

deceive. This withholding of information material to patentability with the intent to deceive the Patent Office constitutes inequitable conduct.

17. During the prosecution of the application leading to the '135 patent, one or more of the people substantively involved in its prosecution were aware of RFC 2401, including Mr. Dannenburg, because it is mentioned in the specification of the '135 patent. Based on Apple's understanding of the allegations by VirnetX, RFC 2401 is material prior art. Nonetheless, those substantively involved in the prosecution of the application intentionally failed to submit this material prior art reference to the Patent Office as required by 37 C.F.R. 1.56 and 37 C.F.R. 1.97, with intent to deceive. Moreover, in mentioning RFC 2401 in the application, those substantively involved in the prosecution of the application described RFC 2401 in a way that concealed its materiality, with intent to deceive. Moreover, the materiality of RFC 2401 leads to an inference of intent to deceive. This conduct, undertaken with the intent to deceive the Patent Office, constitutes inequitable conduct.

18. On or about February 15, 2007, VirnetX filed a lawsuit against Microsoft Corporation ("Microsoft") in the Eastern District of Texas, Tyler Division, C.A. No. 6:07-CV-80 (the "Microsoft Case"), alleging that Microsoft infringed certain VirnetX patents, including the '135 patent.

19. In December 2009, Microsoft filed a reexamination request with the Patent Office requesting reexamination of claims 1-10 and 12 of the '135 patent, citing, among other references, the Aventail reference as prior art under 35 U.S.C. § 102(a). Microsoft asserted that the Aventail reference anticipated claims 1-10 and 12 of the '135 patent.

20. On or about December 31, 2009, the Patent Office ordered reexamination of claims 1-10 and 12 of the '135 patent, finding, in part, that the Aventail reference raised a substantial new question of patentability of all of the requested claims of the '135 patent.

21. On or about January 15, 2010, the Patent Office issued a non-final action rejecting claims 1, 3, 4, 6-10, and 12 of the '135 patent as being anticipated by the Aventail reference.

22. On or about February 22, 2010, VirnetX filed a petition to extend its deadline for responding to the office action, pointing out, in part, that it needed additional time to investigate whether the Aventail reference was proper prior art, including investigating the dates of conception and reduction to practice of the inventions claimed in the '135 patent as well as diligence there between. The petition also cited as a basis for extension that the Microsoft Case was causing a "significant drain" on VirnetX's resources. Moreover, the petition stated that the extension "would likely also permit consideration of any court conclusions regarding the claims presently under reexamination." The petition was filed by Toby Kusmer of McDermott Will & Emery, the same firm that represented VirnetX in the Microsoft Case until 2009. The Patent Office responded on or about February 24, 2010, granting an extension, setting the deadline for response as April 15, 2010.

23. On or about March 8, 2010, trial of the Microsoft Case ("Microsoft Trial") commenced. During the Microsoft Trial, one or more witnesses for VirnetX, including inventor Edward Munger, testified that the claims of the '135 patent were conceived no earlier than three months after September 23, 1999, placing the date of conception for claims 1-10 and 12 on or about December 23, 1999. During the Microsoft Trial, Microsoft alleged, in part, that claims 1-10 and 12 of the '135 patent were anticipated by the Aventail reference, which on information and belief bears a copyright date 1996 – 1999. Microsoft presented evidence indicating that the

Aventail reference may have been published as early as June 1999. Based on a review of the trial record, VirnetX did not dispute the publication date of the Aventail reference. The Microsoft Trial concluded on or about March 16, 2010. Therefore, at least as of March 16, 2010, VirnetX was aware that the Aventail reference may have been published at least as early as June 1999, which is prior to the February 15, 2000, filing date of the application that matured into the '135 patent and prior to the earliest conception date of December 1999 claimed by the inventor of the '135 patent.

24. On or about March 25, VirnetX gave notice to the Patent Office of the outcome of the case and submitted the jury verdict form from the case. On or about March 29, 2010, VirnetX filed a petition requesting that the reexamination proceeding be suspended. The Patent Office did not respond to the request until after the date set for VirnetX's response to the non-final office action rejection.

25. On or about April 15, 2010, VirnetX responded to the office action rejection, in part, by asserting that the Aventail reference should not be considered prior art because no evidence had been submitted by Microsoft that established the actual publication date of the Aventail reference. Moreover, VirnetX did not provide the result of any investigation it may have made with respect to the publication date of the Aventail reference or the dates of conception or reduction to practice of the '135 patent that it indicated it would make in its petition for an extension of time, nor did VirnetX provide any information that it learned from the Microsoft Trial that related to the publication date of the Aventail reference. Based on a review of the prosecution history, VirnetX did not disclose that its conception date for the claims of the '135 patent was no earlier than December 1999, nor did VirnetX disclose that the Aventail

reference may have been published as early as June 1999, as it was made aware of during the Microsoft Trial.

26. On June 16, 2010, the Patent Office issued an Action Closing Prosecution. In the action, the examiner recites that he made an attempt to determine the publication date of the Aventail reference, but was unsuccessful. Based on the lack of evidence of the publication date, the examiner withdrew all of the rejections that had been based on the Aventail reference.

27. VirnetX and/or its representatives, agents, and attorneys who were substantively involved in the prosecution of the reexamination knew or should have known of the Microsoft trial and the evidence presented regarding the publication date of the Aventail reference. For example, Mr. Kusmer specifically referenced the Microsoft Trial and the potential for additional material information to come to light during that trial when seeking an extension to respond to an office action, as set forth in paragraph 24 above. VirnetX and/or its representatives, agents, and attorneys withheld this information with the intent to deceive, either willfully or with such gross negligence or recklessness as constituting an act of willfulness amounting to inequitable conduct. Moreover, the materiality of the Aventail publication and the aforementioned evidence presented at the Microsoft Trial leads to an inference of intent to deceive. Among other things, the information withheld was material to the reexamination of the '135 patent, in violation of the duty of candor the representatives and/or the attorneys owed to the Patent Office.

The '151 Patent

28. The application that issued as the '151 patent was a divisional of the application that issued as the '135 patent.

29. The '151 patent is unenforceable due to unclean hands and/or infectious unenforceability resulting from inequitable conduct committed during the prosecution of the '135 patent, including its reexamination, as set forth above in paragraphs 13-29.

30. The '151 patent is also unenforceable due to inequitable conduct. Based on Apple's understanding of the allegations by VirnetX, one or more of the people substantively involved in the prosecution of the application leading to the '151 patent were aware of information material to the patentability of the claims of the '151 patent, but withheld that information from the Patent Office with the intent to deceive.

31. The withheld information includes the Aventail reference and "Building a Microsoft VPN: A comprehensive collection of Microsoft resources," pages 1-216 ("the Microsoft VPN reference"). These references were material to patentability based upon Apple's understanding of the allegations by VirnetX. This withholding of information material to patentability with the intent to deceive the Patent Office constitutes inequitable conduct.

32. The Aventail and Microsoft VPN references are not cumulative to the prior art made of record during prosecution of the '151 patent. On information and belief, there is a substantial likelihood that a reasonable examiner would have considered this art in determining whether to allow the '151 patent to issue.

33. During the prosecution of the application leading to the '151 patent, one or more of the people substantively involved in its prosecution were aware of the Aventail reference, including Mr. Kusmer of the McDermott law firm. Mr. Kusmer filed the application that led to the issuance of the '151 patent, which was filed on September 20, 2002. The McDermott law firm was aware of the Aventail reference at least as early as February 13, 2008, when Microsoft disclosed the reference in its invalidity contentions. The '151 patent did not issue until February

10, 2009. Based on Apple's understanding of the allegations by VirnetX, the Aventail reference is material prior art. Moreover, in the reexamination of the '135 patent, the Patent Office found a substantial new question of patentability based on the Aventail reference, and the claims of the '135 patent relate to the same subject matter as the claims of the '151 patent. Nonetheless, those substantively involved in the prosecution of the application intentionally failed to disclose this material prior art reference to the Patent Office with intent to deceive. Moreover, the materiality of the Aventail reference leads to an inference of intent to deceive. This conduct, undertaken with the intent to deceive the Patent Office, constitutes inequitable conduct.

34. During the prosecution of the application leading to the '151 patent, one or more of the people substantively involved in its prosecution, including Mr. Kusmer, were aware of the Microsoft VPN reference. The McDermott law firm was aware of the Aventail reference at least as early as February 13, 2008, when Microsoft disclosed the reference in its invalidity contentions. The '151 patent did not issue until February 10, 2009. Based on Apple's understanding of the allegations by VirnetX, the Microsoft VPN reference is material prior art. Moreover, in the reexamination of the '135 patent, the Patent Office found a substantial new question of patentability based on the Microsoft VPN reference, and the claims of the '135 patent relate to the same subject matter as the claims of the '151 patent. Nonetheless, those substantively involved in the prosecution of the application intentionally failed to disclose this material prior art reference to the Patent Office with intent to deceive. Moreover, the materiality of the Microsoft VPN reference leads to an inference of intent to deceive. This conduct, undertaken with the intent to deceive the Patent Office, constitutes inequitable conduct.

JURY DEMAND

35. Apple demands a trial by jury.

EXCEPTIONAL CASE

36. To the extent this is an exceptional case under 35 U.S.C. 285, Apple is entitled to recover from VirnetX for Apples' attorneys' fees and costs incurred in connection with this action.

PRAYER FOR RELIEF

Apple respectfully requests a judgment against VirnetX as follows:

- A. A declaration that Apple does not infringe and has not infringed any valid and enforceable claim of the '135 and '151 patents;
- B. A declaration that the '135 and '151 patents are invalid;
- C. A declaration that the '135 and '151 patents are unenforceable;
- D. That VirnetX take nothing by its Complaint against Apple;
- E. That the Court enter judgment against VirnetX and in favor of Apple and that VirnetX's Complaint be dismissed with prejudice;
- F. That the Court enter a judgment that this is an exceptional case under 35 U.S.C. § 285 and enter a judgment awarding Apple its costs and reasonable attorneys' fees; and
- G. That the Court grant Apple whatever further relief the Court may deem just and proper.

Respectfully submitted,

Date: October 29, 2010

/s/ Danny L. Williams
Danny L. Williams - LEAD ATTORNEY
State Bar No. 21518050
E-mail: danny@wmalaw.com
Ruben S. Bains

Texas Bar No. 24001678
E-mail: rbains@wmalaw.com
Drew Kim
Texas Bar No. 24007482
E-mail: dkim@wmalaw.com
Williams, Morgan & Amerson, P.C.
10333 Richmond, Suite 1100
Houston, Texas 77042
Telephone: (713) 934-7000
Facsimile: (713) 934-7011

ATTORNEYS FOR APPLE INC.

CERTIFICATE OF SERVICE

I hereby certify that the following counsel of record who are deemed to have consented to electronic service are being served this 29th day of October, 2010, with a copy of this document via the Court's CM/ECF system per Local Rule CV-5(a)(3). Any other counsel of record will be served by, electronic mail, facsimile transmission and/or first class mail on this same date.

Dated: October 29, 2010

/s/ Mark Dunglinson
Mark Dunglinson

EXHIBIT D

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION**

VirnetX Inc.,	§	
	§	
Plaintiff,	§	
	§	
v.	§	
	§	CIVIL ACTION NO. 6:10-CV-417 LED
Cisco Systems, Inc.	§	
Apple Inc.	§	Judge: Hon. Leonard Davis
Aastra USA Inc.	§	
Aastra Technologies Ltd.	§	
NEC Corporation, and	§	
NEC Corporation of America,	§	
	§	
Defendants.	§	
	§	

**DEFENDANT AND COUNTERCLAIM-PLAINTIFF AAastra TECHNOLOGIES
LIMITED'S ANSWER, AFFIRMATIVE DEFENSES AND
COUNTERCLAIMS TO VIRNETX INC.'S ORIGINAL COMPLAINT**

Aastra Technologies Limited ("Aastra Technologies"), defendant and counterclaim-plaintiff in the above-entitled and numbered civil action, replies to the Original Complaint of VirnetX Inc. ("VirnetX") as follows.

THE PARTIES

1. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations that VirnetX is "a corporation organized and existing under the laws of the State of Delaware, and maintains its principal place of business at 5615 Scotts Valley Drive, Suite 110 Scotts Valley, California," and, therefore, denies these allegations.

2. Aastra Technologies admits that it is a Canadian corporation with its principal place of business at 155 Snow Blvd., Concord, Ontario Canada, L4K 4N9. Aastra Technologies admits that Aastra USA Inc. is a Delaware corporation with its principal place of business at 2811 Internet Blvd., Frisco, Texas 75034. Aastra Technologies denies that it regularly conducts and transacts business in Texas, throughout the United States, and within the Eastern District of Texas. Aastra Technologies admits that Aastra USA Inc. regularly conducts and transacts business in Texas, throughout the United States, and within the Eastern District of Texas. Aastra Technologies denies that either it or Aastra USA Inc. it has committed or continues to commit any acts that give rise to any cause of action asserted in VirnetX's complaint. Except as admitted above, Aastra Technologies denies the allegations of Paragraph 2.

3. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 3 and therefore, denies these allegations.

4. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 4 and therefore, denies these allegations.

5. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 5 and therefore, denies these allegations.

JURISDICTION AND VENUE

6. Aastra Technologies admits that VirnetX purports to bring this action under the patent laws of the United States, Title 35, United States Code, but Aastra Technologies denies any liability thereunder. Aastra Technologies does not contest that the Court has exclusive subject matter over this matter under 28 U.S.C. § 1338. Except as admitted above, Aastra Technologies denies the allegations of Paragraph 6.

7. Admitted.

8. Aastra Technologies admits that this Court has personal jurisdiction over Aastra Technologies. Except as admitted above, Aastra Technologies denies the allegations of Paragraph 8.

ASSERTED PATENTS

9. Aastra Technologies admits that United States Patent No. 6,502,135 (“the ‘135 patent”), entitled “Agile Network Protocol for Secure Communications with Assured System Availability” issued on December 31, 2002, but denies any further characterization of the ‘135 patent, its inventors, or its examination as alleged in Paragraph 9. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations that VirnetX is the “owner of all rights, title, and interest in and to the ‘135 patent and possesses all rights of recovery under the ‘135 patent” and, therefore, denies these allegations. Aastra Technologies admits that a purported copy of the ‘135 patent was attached to the complaint as Exhibit A. Except as expressly admitted above, Aastra Technologies denies the allegations in Paragraph 9.

10. Aastra Technologies admits that United States Patent No. 6,839,759 (“the ‘759 patent”), entitled “Method for Establishing Secure Communication Link

Between Computers of Virtual Private Network Without User Entering Any Cryptographic Information” issued on January 4, 2005, but denies any further characterization of the ‘759 patent, its inventors, or its examination as alleged in Paragraph 10. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations that VirnetX is the “owner of all rights, title, and interest in and to the ‘759 patent and possesses all rights of recovery under the ‘759 patent” and, therefore, denies these allegations. Aastra Technologies admits that a purported copy of the ‘759 patent was attached to the complaint as Exhibit B. Except as expressly admitted above, Aastra Technologies denies the allegations in Paragraph 10.

11. Aastra Technologies admits that United States Patent No. 7,188,180 (“the ‘180 patent”), entitled “Method for Establishing Secure Communications Link Between Computers of Virtual Private Network” issued on March 6, 2007, but denies any further characterization of the ‘180 patent, its inventors, or its examination as alleged in Paragraph 11. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations that VirnetX is the “owner of all rights, title, and interest in and to the ‘180 patent and possesses all rights of recovery under the ‘180 patent” and, therefore, denies these allegations. Aastra Technologies admits that a purported copy of the ‘180 patent was attached to the complaint as Exhibit C. Except as expressly admitted above, Aastra Technologies denies the allegations in Paragraph 11.

12. Aastra Technologies admits that United States Patent No. 7,418,504 (“the ‘504 patent”), entitled “Agile Network Protocol for Secure Communications Using

Secure Domain Names” issued on August 26, 2008, but denies any further characterization of the ‘504 patent, its inventors, or its examination as alleged in Paragraph 12. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations that VirnetX is the “owner of all rights, title, and interest in and to the ‘504 patent and possesses all rights of recovery under the ‘504 patent” and, therefore, denies these allegations. Aastra Technologies admits that a purported copy of the ‘504 patent was attached to the complaint as Exhibit D. Except as expressly admitted above, Aastra Technologies denies the allegations in Paragraph 12.

13. Aastra Technologies admits that United States Patent No. 7,490,151 (“the ‘151 patent”), entitled “Establishment of a Secure Communication Link Based on a Domain Name Service (DNS) Request” issued on February 10, 2009, but denies any further characterization of the ‘151 patent, its inventors, or its examination as alleged in Paragraph 13. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations that VirnetX is the “owner of all rights, title, and interest in and to the ‘151 patent and possesses all rights of recovery under the ‘151 patent” and, therefore, denies these allegations. Aastra Technologies admits that a purported copy of the ‘151 patent was attached to the complaint as exhibit E. Except as expressly admitted above, Aastra Technologies denies the allegations in Paragraph 13.

COUNT ONE

PATENT INFRINGEMENT BY AASTRA TECHNOLOGIES

14. Aastra Technologies incorporates by reference paragraphs 1-13 as if fully set forth herein. Aastra Technologies denies that it has infringed and/or continues to infringe the '135 patent.

15. Denied.

16. Denied.

17. Denied.

18. Denied.

19. Denied.

20. Denied.

21. Denied.

22. Aastra Technologies admits that it has received actual notice of infringement by virtue of the filing of this lawsuit. Aastra Technologies denies that it has received constructive notice. Aastra Technologies denies that VirnetX has complied with the requirements of 35 U.S.C. § 287. Except as expressly admitted above, Aastra Technologies denies the allegations in Paragraph 22.

COUNT TWO

PATENT INFRINGEMENT BY APPLE

23. Aastra Technologies incorporates by reference paragraphs 1-22 as if fully set forth herein. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 23 and therefore, denies these allegations.

24. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 24 and therefore, denies these allegations.

25. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 25 and therefore, denies these allegations.

26. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 26 and therefore, denies these allegations.

27. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 27 and therefore, denies these allegations.

28. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 28 and therefore, denies these allegations.

29. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 29 and therefore, denies these allegations.

30. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 30 and therefore, denies these allegations.

31. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 31 and therefore, denies these allegations.

32. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 32 and therefore, denies these allegations.

33. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 33 and therefore, denies these allegations.

34. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 34 and therefore, denies these allegations.

35. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 35 and therefore, denies these allegations.

36. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 36 and therefore, denies these allegations.

COUNT THREE

PATENT INFRINGEMENT BY CISCO

37. Aastra Technologies incorporates by reference paragraphs 1-36 as if fully set forth herein. Aastra Technologies is without knowledge or information sufficient

to form a belief as to the truth of the allegations set forth in Paragraph 37 and therefore, denies these allegations.

38. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 38 and therefore, denies these allegations.

39. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 39 and therefore, denies these allegations.

40. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 40 and therefore, denies these allegations.

41. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 41 and therefore, denies these allegations.

42. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 42 and therefore, denies these allegations.

43. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 43 and therefore, denies these allegations.

44. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 44 and therefore, denies these allegations.

45. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 45 and therefore, denies these allegations.

46. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 46 and therefore, denies these allegations.

47. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 47 and therefore, denies these allegations.

48. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 48 and therefore, denies these allegations.

49. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 49 and therefore, denies these allegations.

50. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 50 and therefore, denies these allegations.

51. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 51 and therefore, denies these allegations.

52. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 52 and therefore, denies these allegations.

53. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 53 and therefore, denies these allegations.

54. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 54 and therefore, denies these allegations.

55. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 55 and therefore, denies these allegations.

56. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 56 and therefore, denies these allegations.

57. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 57 and therefore, denies these allegations.

58. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 58 and therefore, denies these allegations.

59. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 59 and therefore, denies these allegations.

60. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 60 and therefore, denies these allegations.

61. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 61 and therefore, denies these allegations.

62. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 62 and therefore, denies these allegations.

63. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 63 and therefore, denies these allegations.

COUNT FOUR

PATENT INFRINGEMENT BY NEC

64. Aastra Technologies incorporates by reference paragraphs 1-63 as if fully set forth herein. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 64 and therefore, denies these allegations.

65. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 65 and therefore, denies these allegations.

66. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 66 and therefore, denies these allegations.

67. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 67 and therefore, denies these allegations.

68. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 68 and therefore, denies these allegations.

69. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 69 and therefore, denies these allegations.

70. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 70 and therefore, denies these allegations.

71. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 71 and therefore, denies these allegations.

72. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 72 and therefore, denies these allegations.

73. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 73 and therefore, denies these allegations.

74. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 74 and therefore, denies these allegations.

75. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 75 and therefore, denies these allegations.

76. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 76 and therefore, denies these allegations.

77. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 77 and therefore, denies these allegations.

AASTRA TECHNOLOGIES' AFFIRMATIVE DEFENSES

78. Aastra Technologies has not and does not literally, directly, contributorily, by way of inducement, and/or under the doctrine of equivalents, infringe any valid and/or enforceable claim of the '135 patent.

79. Each of the claims of the '135 patent are invalid for failing to comply with one of more of the requirements for patentability specified by Part II of Title 35 of the United States Code §101 *et seq.*, including without limitation 35 U.S.C. §§ 102, 103 and/or 112.

80. VirnetX is estopped from construing the claims of the '135 patent to cover or include, either literally or by application of the doctrine of equivalents, methods used, devices manufactured, used, imported, sold or offered for sale by Aastra Technologies because of admissions and statements to the PTO during prosecution of the applications leading to the issuance of the patent, disclosure or language in the specification of the patent and/or limitations in the claims of the patent.

81. The relief sought by VirnetX is barred in whole or in part by the doctrine of laches.

82. To the extent that products accused of infringement were or are used or manufactured by or for the United States, the relief sought by VirnetX is limited by 28 U.S.C. § 1498(a).

83. The relief sought by VirnetX is barred in whole or in part by 35 U.S.C. § 287.

84. VirnetX is not entitled to an injunction against Aastra Technologies because VirnetX has an adequate remedy at law.

85. VirnetX lacks standing to bring suit to enforce the '135 patent because it does not possess all substantial rights in the '135 patent.

86. The '135 patent is unenforceable due to inequitable conduct. Based on the contents of the prosecution history and based on Aastra Technologies' understanding

of the allegations by VirnetX, one or more of the people substantively involved in the prosecution of the application leading to the '135 patent, and the subsequent reexamination of the '135 patent, were aware of information material to the patentability of the claims of the '135 patent, but withheld that information from the Patent Office with the intent to deceive.

The existence of US. Patent Application No. 09/399,753 ("the Miller Application"), was withheld during the prosecution of the '135 patent. The pendency of the Miller Application was information material to patentability of the '135 patent based on Aastra Technologies' understanding of the allegations by VirnetX. The withheld information also includes RFC 2401-Security Architecture for the Internet Protocol ("RFC 2401") and the Aventail Administrator's Guide ("Aventail"), which are material to patentability based upon Aastra Technologies' understanding of the allegations by VirnetX. This withholding of information material to patentability with the intent to deceive the Patent Office constitutes inequitable conduct.

The Miller Application, RFC 2401, and the Aventail reference are not cumulative to the prior art made of record during prosecution of the '135 patent. There is a substantial likelihood that a reasonable examiner would have considered this art in determining whether to allow the '135 patent to issue.

During the prosecution of the application leading to the '135 patent, one or more of the people substantively involved in its prosecution (including Ross Dannenburg) were aware of the Miller Application. Mr. Dannenburg was involved in the prosecution of the Miller Application during the prosecution of the '135 patent at least as early as June 14, 2002, when he signed an Amendment / Response in the

prosecution history of the Miller Application. Mr. Dannenburg was involved in the prosecution of the '135 patent at least as early as January 28, 2002, when he signed a Transmittal Form for an Amendment / Response in the prosecution file history of the '135 patent. Therefore, Mr. Dannenburg was involved in the prosecution of the Miller Application while he was prosecuting the '135 patent. Based on Aastra Technologies' understanding of the allegations by VirnetX, the pendency of the Miller Application is information material to patentability. Nonetheless, those substantively involved in the prosecution of the application intentionally failed to disclose this material information to the Patent Office at any time during the prosecution of the '135 patent with intent to deceive. Moreover, the materiality of the Miller Application leads to an inference of intent to deceive. This withholding of information material to patentability with the intent to deceive the Patent Office constitutes inequitable conduct.

During the prosecution of the application leading to the '135 patent, one or more of the people substantively involved in its prosecution were aware of RFC 2401, including Mr. Dannenburg, because it is mentioned in the specification of the '135 patent. Based on Aastra Technologies' understanding of the allegations by VirnetX, RFC 2401 is material prior art. Nonetheless, those substantively involved in the prosecution of the application intentionally failed to submit this material prior art reference to the Patent Office as required by 37 C.F.R. 1.56 and 37 C.F.R. 1.97, with intent to deceive. Moreover, in mentioning RFC 2401 in the application, those substantively involved in the prosecution of the application described RFC 2401 in a way that concealed its materiality, with intent to deceive. Moreover, the materiality of

RFC 2401 leads to an inference of intent to deceive. This conduct, undertaken with the intent to deceive the Patent Office, constitutes inequitable conduct.

VirnetX also committed inequitable conduct during the reexamination of the '135 patent. On or about February 15, 2007, VirnetX filed a lawsuit against Microsoft Corporation ("Microsoft") in the Eastern District of Texas, Tyler Division, C.A. No. 6:07-CV-80 (the "Microsoft trial"), alleging that Microsoft infringed certain VirnetX patents, including the '135 patent.

During the Microsoft trial, one or more witnesses for VirnetX, including inventor Edward Munger, testified that the claims of the '135 patent were conceived no earlier than three months after September 23, 1999, placing the date of conception for claims 1-10 and 12 on or after December 23, 1999.

During the Microsoft trial, Microsoft alleged, in part, that claims 1-10 and 12 of the '135 patent were anticipated by the Aventail reference, which on information and belief bears a copyright date between 1996 – 1999.

In December 2009, Microsoft filed a re-examination request with the Patent Office requesting re-examination of claims 1-10 and 12 of the '135 patent, citing, among other references, the Aventail reference as prior art under 35 U.S.C. § 102(a). Microsoft asserted that the Aventail reference anticipated claims 1-10 and 12 of the '135 patent.

On or about December 31, 2009, the Patent Office ordered re-examination of claims 1-10 and 12 of the '135 patent, finding, in part, that the Aventail reference raised a substantial new question of patentability of all of the requested claims of the '135 patent.

On or about January 15, 2010, the Patent Office issued a non-final action rejecting claims 1, 3, 4, 6-10, and 12 as being anticipated by the Aventail reference.

On or about February 22, 2010, VirnetX filed a petition to extend its deadline for responding to the office action, pointing out, in part, that it needed additional time to investigate whether the Aventail reference was proper prior art, including investigating the dates of conception and reduction to practice of the inventions claimed in the '135 patent as well as diligence there between. The petition also cited as a basis for extension that the Microsoft case was causing a "significant drain" on VirnetX's resources. Moreover, the petition stated that the extension "would likely also permit consideration of any court conclusions regarding the claims presently under reexamination." The petition was filed by Toby Kusmer of McDermott Will & Emery, the same firm that represented VirnetX in the Microsoft case until 2009. The Patent Office responded on or about February 24, 2010, granting an extension, and setting the deadline for response as April 15, 2010.

On or about March 8, 2010, the Microsoft trial commenced. During trial, Microsoft argued that the Aventail reference invalidated claims 1-10 and 12 of the '135 patent. Microsoft presented evidence indicating that the Aventail reference may have been published as early as June 1999. Based on a review of the trial record, VirnetX did not dispute the publication date of the Aventail reference. The Microsoft trial concluded on or about March 16, 2010. Therefore, at least as of March 16, 2010, VirnetX was aware that the Aventail reference may have been published at least as early as June 1999, which is prior to the February 15, 2000, filing date of the application that matured into the '135 patent and prior to the earliest conception date

of December 1999 claimed by the inventor of the '135 patent.

On or about March 25, 2010, VirnetX gave notice to the Patent Office of the outcome of the case and submitted the jury verdict form from the case. On or about March 29, 2010, VirnetX filed a petition requesting that the re-examination proceeding be suspended. The Patent Office did not respond to the request until after the date set for VirnetX's response to the non-final office action rejection.

On or about April 15, 2010, VirnetX responded to the office action rejection, in part, by asserting that the Aventail reference should not be considered prior art because no evidence had been submitted by Microsoft that established the actual publication date of the Aventail reference. Moreover, VirnetX did not provide the result of any investigation it may have made with respect to the publication date of the Aventail reference or the dates of conception or reduction to practice of the '135 patent that it indicated it would make in its petition for an extension of time, nor did VirnetX provide any information that it learned from the Microsoft trial that related to the publication date of the Aventail reference. Based on a review of the prosecution history, VirnetX did not disclose that its conception date for the claims of the '135 patent was no earlier than December 1999, nor did VirnetX disclose that the Aventail reference may have been published as early as June 1999, a fact to which VirnetX was made aware during the Microsoft trial.

On June 16, 2010, the Patent Office issued an Action Closing Prosecution. In the action, the examiner recites that he made an attempt to determine the publication date of the Aventail reference, but was unsuccessful. Based on the lack of evidence of the publication date, the examiner withdrew all of the rejections that had

been based on the Aventail reference.

VirnetX and/or its representatives, agents, and attorneys who were substantively involved in the prosecution of the re-examination knew or should have known of the Microsoft trial and the evidence presented regarding the publication date of the Aventail reference. For example, Mr. Kusmer specifically referenced the Microsoft trial and the potential for additional material information to come to light during that trial when seeking an extension to respond to an office action, as set forth above. VirnetX and/or its representatives, agents, and attorneys withheld this information with the intent to deceive, either willfully or with such gross negligence or recklessness as constituting an act of willfulness amounting to inequitable conduct. Moreover, the high degree of materiality of the Aventail publication and the aforementioned evidence presented at the Microsoft trial leads to an inference of intent to deceive. Among other things, the information withheld was material to the reexamination of the '135 patent, in violation of the duty of candor the representatives and/or the attorneys owed to the Patent Office.

AASTRA TECHNOLOGIES' COUNTERCLAIMS

87. Aastra Technologies Limited ("Aastra Technologies") is a Canadian corporation with its principal place of business at 155 Snow Blvd., Concord, Ontario Canada, L4K 4N9.

88. VirnetX, Inc. ("VirnetX"), as represented in Paragraph 1 of its Original Complaint, has claimed that it is a Delaware corporation with its principal place of business at 5615 Scotts Valley Drive, Suite 110 Scotts Valley, California.

89. This Court has subject matter jurisdiction over the Counterclaim pursuant to 28 U.S.C. §§ 1331, 1338, and 2201 as it arises under an Act of Congress relating to patents.

90. Venue is proper in this district under 28 U.S.C. §§ 1391(b), (c) and 1400.

91. By filing its complaint, VirnetX has consented to the personal jurisdiction of this Court.

DECLARATORY JUDGMENT FOR NON-INFRINGEMENT OF UNITED STATES PATENT NO. 6,502,135

92. Aastra Technologies hereby re-alleges and incorporates by reference Paragraphs 87-91 as though fully set forth herein.

93. United States Patent No. 6,502,135 (“the ‘135 patent”), entitled “Agile Network Protocol for Secure Communications with Assured System Availability” was issued on December 31, 2002. VirnetX claims to be the owner by assignment of the ‘135 patent.

94. Aastra Technologies has not directly infringed, contributed to infringement, or induced infringement of any valid claim of the ‘135 patent, nor is Aastra Technologies directly infringing, contributing to infringement, or inducing infringement of any valid claim of the ‘135 patent.

95. An actual controversy exists between Aastra Technologies and VirnetX regarding the alleged infringement ‘135 patent by virtue of VirnetX’s allegation of infringement.

96. Aastra Technologies is entitled to judgment from this Court that the ‘135 patent is not infringed by Aastra Technologies.

**DECLARATORY JUDGMENT FOR INVALIDITY OF UNITED STATES
PATENT NO. 6,502,135**

97. Aastra Technologies hereby re-alleges and incorporates by reference Paragraphs 87-96 as though fully set forth herein.

98. The '135 patent is invalid for failing to comply with one or more of the requirements for patentability set forth in Part II of Title 35 U.S.C. § 101 *et seq.*, including without limitation 35 U.S.C. §§102, 103 and/or 112.

99. An actual controversy exists between Aastra Technologies and VirnetX regarding the validity of the '135 patent by virtue of VirnetX's allegation of infringement.

100. Aastra Technologies is entitled to judgment from this Court that the '135 patent is invalid.

**DECLARATORY JUDGMENT FOR UNENFORCEABILITY OF UNITED
STATES PATENT NO. 6,502,135**

101. Aastra Technologies hereby re-alleges and incorporates by reference Paragraphs 87-100 as though fully set forth herein.

102. The '135 patent is unenforceable due to inequitable conduct. Based on the contents of the prosecution history and based on Aastra Technologies' understanding of the allegations by VirnetX, one or more of the people substantively involved in the prosecution of the application leading to the '135 patent, and the subsequent reexamination of the '135 patent, were aware of information material to the patentability of the claims of the '135 patent, but withheld that information from the Patent Office with the intent to deceive.

103. The existence of US. Patent Application No. 09/399,753 ("the Miller Application"), was withheld during the prosecution of the '135 patent. The pendency of the Miller Application was information material to patentability of the '135 patent based on Aastra Technologies' understanding of the allegations by VirnetX. The withheld information also includes RFC 2401-Security Architecture for the Internet Protocol ("RFC 2401") and the Aventail Administrator's Guide ("Aventail"), which are material to patentability based upon Aastra Technologies' understanding of the allegations by VirnetX. This withholding of information material to patentability with the intent to deceive the Patent Office constitutes inequitable conduct.

104. The Miller Application, RFC 2401, and the Aventail reference are not cumulative to the prior art made of record during prosecution of the '135 patent. There is a substantial likelihood that a reasonable examiner would have considered this art in determining whether to allow the '135 patent to issue.

105. During the prosecution of the application leading to the '135 patent, one or more of the people substantively involved in its prosecution (including Ross Dannenburg) were aware of the Miller Application. Mr. Dannenburg was involved in the prosecution of the Miller Application during the prosecution of the '135 patent at least as early as June 14, 2002, when he signed an Amendment / Response in the prosecution history of the Miller Application. Mr. Dannenburg was involved in the prosecution of the '135 patent at least as early as January 28, 2002, when he signed a Transmittal Form for an Amendment / Response in the prosecution file history of the '135 patent. Therefore, Mr. Dannenburg was involved in the prosecution of the Miller Application while he was prosecuting the '135 patent. Based on Aastra

Technologies' understanding of the allegations by VirnetX, the pendency of the Miller Application is information material to patentability. Nonetheless, those substantively involved in the prosecution of the application intentionally failed to disclose this material information to the Patent Office at any time during the prosecution of the '135 patent with intent to deceive. Moreover, the materiality of the Miller Application leads to an inference of intent to deceive. This withholding of information material to patentability with the intent to deceive the Patent Office constitutes inequitable conduct.

106. During the prosecution of the application leading to the '135 patent, one or more of the people substantively involved in its prosecution were aware of RFC 2401, including Mr. Dannenburg, because it is mentioned in the specification of the '135 patent. Based on Aastra Technologies' understanding of the allegations by VirnetX, RFC 2401 is material prior art. Nonetheless, those substantively involved in the prosecution of the application intentionally failed to submit this material prior art reference to the Patent Office as required by 37 C.F.R. 1.56 and 37 C.F.R. 1.97, with intent to deceive. Moreover, in mentioning RFC 2401 in the application, those substantively involved in the prosecution of the application described RFC 2401 in a way that concealed its materiality, with intent to deceive. Moreover, the materiality of RFC 2401 leads to an inference of intent to deceive. This conduct, undertaken with the intent to deceive the Patent Office, constitutes inequitable conduct.

107. VirnetX also committed inequitable conduct during the reexamination of the '135 patent. On or about February 15, 2007, VirnetX filed a lawsuit against Microsoft Corporation ("Microsoft") in the Eastern District of Texas, Tyler Division,

C.A. No. 6:07-CV-80 (the “Microsoft trial”), alleging that Microsoft infringed certain VirnetX patents, including the ‘135 patent.

108. During the Microsoft trial, one or more witnesses for VirnetX, including inventor Edward Munger, testified that the claims of the ‘135 patent were conceived no earlier than three months after September 23, 1999, placing the date of conception for claims 1-10 and 12 on or after December 23, 1999.

109. During the Microsoft trial, Microsoft alleged, in part, that claims 1-10 and 12 of the ‘135 patent were anticipated by the Aventail reference, which on information and belief bears a copyright date between 1996 – 1999.

110. In December 2009, Microsoft filed a reexamination request with the Patent Office requesting re-examination of claims 1-10 and 12 of the ‘135 patent, citing, among other references, the Aventail reference as prior art under 35 U.S.C. § 102(a). Microsoft asserted that the Aventail reference anticipated claims 1-10 and 12 of the ‘135 patent.

111. On or about December 31, 2009, the Patent Office ordered re-examination of claims 1-10 and 12 of the ‘135 patent, finding, in part, that the Aventail reference raised a substantial new question of patentability of all of the requested claims of the ‘135 patent.

112. On or about January 15, 2010, the Patent Office issued a non-final action rejecting claims 1, 3, 4, 6-10, and 12 as being anticipated by the Aventail reference.

113. On or about February 22, 2010, VirnetX filed a petition to extend its deadline for responding to the office action, pointing out, in part, that it needed additional time to investigate whether the Aventail reference was proper prior art.

including investigating the dates of conception and reduction to practice of the inventions claimed in the '135 patent as well as diligence there between. The petition also cited as a basis for extension that the Microsoft case was causing a "significant drain" on VirnetX's resources. Moreover, the petition stated that the extension "would likely also permit consideration of any court conclusions regarding the claims presently under reexamination." The petition was filed by Toby Kusmer of McDermott Will & Emery, the same firm that represented VirnetX in the Microsoft case until 2009. The Patent Office responded on or about February 24, 2010, granting an extension, and setting the deadline for response as April 15, 2010.

114. On or about March 8, 2010, the Microsoft trial commenced. During trial, Microsoft argued that the Aventail reference invalidated claims 1-10 and 12 of the '135 patent. Microsoft presented evidence indicating that the Aventail reference may have been published as early as June 1999. Based on a review of the trial record, VirnetX did not dispute the publication date of the Aventail reference. The Microsoft trial concluded on or about March 16, 2010. Therefore, at least as of March 16, 2010, VirnetX was aware that the Aventail reference may have been published at least as early as June 1999, which is prior to the February 15, 2000, filing date of the application that matured into the '135 patent and prior to the earliest conception date of December 1999 claimed by the inventor of the '135 patent.

115. On or about March 25, 2010, VirnetX gave notice to the Patent Office of the outcome of the case and submitted the jury verdict form from the case. On or about March 29, 2010, VirnetX filed a petition requesting that the re-examination

proceeding be suspended. The Patent Office did not respond to the request until after the date set for VirnetX's response to the non-final office action rejection.

116. On or about April 15, 2010, VirnetX responded to the office action rejection, in part, by asserting that the Aventail reference should not be considered prior art because no evidence had been submitted by Microsoft that established the actual publication date of the Aventail reference. Moreover, VirnetX did not provide the result of any investigation it may have made with respect to the publication date of the Aventail reference or the dates of conception or reduction to practice of the '135 patent that it indicated it would make in its petition for an extension of time, nor did VirnetX provide any information that it learned from the Microsoft trial that related to the publication date of the Aventail reference. Based on a review of the prosecution history, VirnetX did not disclose that its conception date for the claims of the '135 patent was no earlier than December 1999, nor did VirnetX disclose that the Aventail reference may have been published as early as June 1999, a fact to which VirnetX was made aware during the Microsoft trial.

117. On June 16, 2010, the Patent Office issued an Action Closing Prosecution. In the action, the examiner recites that he made an attempt to determine the publication date of the Aventail reference, but was unsuccessful. Based on the lack of evidence of the publication date, the examiner withdrew all of the rejections that had been based on the Aventail reference.

118. VirnetX and/or its representatives, agents, and attorneys who were substantively involved in the prosecution of the re-examination knew or should have known of the Microsoft trial and the evidence presented regarding the publication

date of the Aventail reference. For example, Mr. Kusmer specifically referenced the Microsoft trial and the potential for additional material information to come to light during that trial when seeking an extension to respond to an office action, as set forth above. VirnetX and/or its representatives, agents, and attorneys withheld this information with the intent to deceive, either willfully or with such gross negligence or recklessness as constituting an act of willfulness amounting to inequitable conduct. Moreover, the high degree of materiality of the Aventail publication and the aforementioned evidence presented at the Microsoft trial leads to an inference of intent to deceive. Among other things, the information withheld was material to the reexamination of the '135 patent, in violation of the duty of candor the representatives and/or the attorneys owed to the Patent Office.

EXCEPTIONAL CASE

119. This is an exceptional case pursuant to 35 U.S.C. § 285 entitling Aastra Technologies to an award of attorneys' fees as a result of, *inter alia*, VirnetX's assertion of the '135 patent against Aastra Technologies with the knowledge that the '135 patent is unenforceable and for VirnetX's failure to perform a reasonable pre-suit investigation of its infringement contentions against Aastra Technologies.

DEMAND FOR JURY TRIAL

120. Aastra Technologies hereby demands a jury for all issues so triable.

PRAYER FOR RELIEF

121. WHEREFORE, Aastra Technologies prays for the following relief:

- A. That the Court enter judgment that VirnetX is not entitled to any relief with respect to its allegations against Aastra Technologies and dismiss all of VirnetX's allegations with prejudice;
- B. That the Court enter a judgment that Aastra has not infringed and is not directly infringing or indirectly infringing by contribution or inducement, whether willfully or otherwise, any claim of the '135 patent, as alleged by VirnetX;
- C. That the Court enter a judgment that the claims of the '135 patent are invalid;
- D. That the Court enter a judgment that the claims of the '135 patent are unenforceable;
- E. That the Court enter a declaratory judgment that the claims of the '135 patent are not infringed;
- F. That the Court enter a declaratory judgment that the claims of the '135 patent are invalid;
- G. That the Court enter a declaratory judgment that the claims of the '135 patent are unenforceable;
- H. That the Court declare this an exceptional case and award Aastra Technologies its costs, expenses, and reasonable attorneys' fees pursuant to 35 U.S.C. § 285 and all other applicable statutes, rules, and common law;
and

1. That the Court award Aastra Technologies such other and further relief as the Court may deem just and proper.

DATED: October 29, 2010

Respectfully Submitted,

By: /s/ Phillip N. Cockrell

Phillip N. Cockrell

Lead Attorney

State Bar No. 04465500

pcockrell@pattonroberts.com

PATTON ROBERTS, PLLC

400 Century Plaza

2900 St. Michael Dr.

Texarkana, Texas 75503

Telephone: 903-334-7000

Facsimile: 903-334-7007

Jon B. Hyland

jhyland@pattonroberts.com

State Bar No. 24046131

Robert D. Katz

rkatz@pattonroberts.com

State Bar No. 24057936

PATTON ROBERTS, PLLC

901 Main St., Suite 3300

Dallas, Texas 75202

Telephone: 214-580-3826

Facsimile: 903-334-7007

CERTIFICATE OF SERVICE

This is to certify that all counsel of record who are deemed to have consented to electronic service are being served with a copy of this document via the Court's CM/ECF system per Local Rule CV-5(a)(3) on this the 29th Day of October, 2010.

/s/ Phillip N. Cockrell

EXHIBIT F1

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

VIRNETX * Civil Docket No.
* 6:07-CV-80
VS. * Tyler, Texas
*
* March 8, 2010
MICROSOFT CORPORATION * 8:45 A.M.

TRANSCRIPT OF JURY TRIAL
BEFORE THE HONORABLE JUDGE LEONARD DAVIS
UNITED STATES DISTRICT JUDGE

APPEARANCES:

FOR THE PLAINTIFFS: MR. DOUGLAS CAWLEY
MR. BRADLEY CALDWELL
MR. JASON D. CASSADY
MR. LUKE MCLEROY
McKool-Smith
300 Crescent Court
Suite 1500
Dallas, TX 75201

MR. ROBERT M. PARKER
Parker, Bunt & Ainsworth
100 East Ferguson
Suite 1114
Tyler, TX 75702

APPEARANCES CONTINUED ON NEXT PAGE:

COURT REPORTERS: MS. SUSAN SIMMONS, CSR
Ms. Judith Werlinger, CSR
Official Court Reporters
100 East Houston, Suite 125
Marshall, TX 75670
903/935-3868

(Proceedings recorded by mechanical stenography,
transcript produced on CAT system.)

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

APPEARANCES CONTINUED:

FOR THE DEFENDANT:

MR. MATTHEW POWERS
MR. JARED BOBROW
MR. PAUL EHRLICH
MR. THOMAS KING
MR. ROBERT GERRITY
Weil Gotshal & Manges
201 Redwood Shores Parkway
5th Floor
Redwood City, CA 94065

MS. ELIZABETH WEISWASSER
MR. TIM DeMASI
Weil Gotshal & Manges
767 Fifth Avenue
New York, NY 10153

MR. DANIEL BOOTH
Weil Gotshal & Manges
700 Louisiana
Suite 1600
Houston, TX 77002

MR. RICHARD SAYLES
MR. MARK STRACHAN
Sayles Werbner
1201 Elm Street
4400 Renaissance Tower
Dallas, TX 75270

MR. ERIC FINDLAY
Findlay Craft
6760 Old Jacksonville Highway
Suite 101
Tyler, TX 75703

* * * * *

P R O C E E D I N G S

(Jury out.)

COURT SECURITY OFFICER: All rise.

THE COURT: Please be seated. All right

Ms. Ferguson, if you'll call the case.

1 COURTROOM DEPUTY: Case No. 6:07-cv-80,
2 VirnetX versus Microsoft.

3 THE COURT: All right. Announcements?

4 MR. CAWLEY: Good morning, Your Honor.
5 The Plaintiff VirnetX is ready.

6 THE COURT: Okay.

7 MR. POWERS: Good morning, Your Honor.
8 Microsoft is ready as well.

9 THE COURT: Very well.

10 My goodness, we have a big audience
11 today.

12 All right. Do we have some matters to
13 take up with the Court before we bring the jury in?

14 MR. POWERS: Yes, Your Honor, just a few.

15 The first relates to the claims at issue
16 which VirnetX has dropped at pretrial. There's three of
17 them, and we just wanted it to be on the record that
18 those are dropped with prejudice. And I understand
19 VirnetX has no objection to that.

20 The three are, first, Claim 7 of the '135
21 patent; second, the allegations of contributory
22 infringement as to the '180 patent; and, third, the
23 allegations with regard to the '135 patent against the
24 PeerNet APIs.

25 THE COURT: Is that correct, that VirnetX

1 dismisses those with prejudice?

2 MR. McLEROY: Yes, Your Honor.

3 THE COURT: Okay. Very well.

4 What else?

5 MR. POWERS: The second, Your Honor, is
6 the stipulation which was filed by the parties last
7 night regarding objections to certain exhibits. I have
8 a copy for you, if it's not immediately available.

9 The parties just thought that would be an
10 easier way of handling that issue outside the presence
11 of the jury.

12 THE COURT: I want to look at that, and I
13 want to hear some just discussion as to what that is.
14 Lots of times on those, I like a final bite at the apple
15 in the context of hearing the testimony, if it's
16 something that you're really serious about wanting to
17 put in, and you think it's important to the case.
18 But maybe y'all can explain it to me such that we don't
19 need to do that. But let's -- I don't want to keep the
20 jury waiting, so we'll take that up later.

21 MR. POWERS: With that, I think there's
22 only one more issue that probably needs to be discussed
23 today before the jury, and that's a question about how
24 Your Honor wishes to handle the admission of exhibits.
25 The parties are agreed in all respects with respect to

1 how we would enforce your order with one exception. The
2 exception is this: That VirnetX has given us a list
3 last night of 260-some-odd exhibits that they wish to
4 have admitted en masse this morning. And as to those
5 exhibits where -- where there's no objection, we have no
6 objection with one exception.

7 And that is as to exhibits where there's
8 no intended use with a witness, that is inconsistent, as
9 we understand it, with Your Honor's pretrial order,
10 which said, for example, you can use an exhibit in
11 opening where there's no objection as long as you have a
12 good-faith intent to use it with a witness or that it
13 will be used with a witness.

14 Our concern is that the proposal advanced
15 by VirnetX would unduly burden the jury and the Court
16 with perhaps hundreds of exhibits that no witness would
17 ever explain or discuss.

18 And our view of Your Honor's past
19 practice and appropriate practice is that, of course, we
20 could admit exhibits en masse before the jury gets here
21 as to which there is no objection. That's the procedure
22 we followed in i4i, and we certainly agree with that.

23 But not just dumping into the record
24 hundreds of exhibits that no witness is ever going to
25 discuss, and that's the dispute before Your Honor at

1 this point.

2 MR. McLEROY: Yes, Your Honor, there's a
3 long list of unobjected to exhibits, and we're aware of
4 Your Honor's concern about the length of trial. And we
5 don't want to burden the testimony, particularly the
6 testimony of our infringement expert, by having him
7 handle a number of exhibits that we believe we need in
8 the record for appeal that are only going to slow down
9 Your Honor's trial.

10 THE COURT: Well, what my goal is, is to
11 speed the trial up. If -- I mean, an exhibit can be
12 admitted without a witness referring to it. I mean, if
13 it's otherwise admissible and is -- so my ruling would
14 be that they can preadmit everything that is -- that
15 there's no objection to, and that -- and if there is no
16 objection and it's admissible.

17 Now, if you want to object to some of
18 them and put them through the paces of proving them up,
19 I mean, that's your right to do so.

20 MR. POWERS: No, that wasn't our concern.
21 We have no objection -- we have no desire to force them
22 to go through the issue of proving them up. That's not
23 the point. We have no objection to any of these
24 exhibits.

25 Our concern is that if the record has

1 literally hundreds of exhibits that no witness has ever
2 discussed, that that is something that is not fair to
3 the jury or Your Honor, because when those exhibits are
4 then used, and, presumably, they're being put into the
5 record to be used either on appeal or in argument to the
6 jury or in argument to Your Honor, the jury and Your
7 Honor don't have the benefit of testimony about what
8 that exhibit means and doesn't mean.

9 And often, an exhibit will say something
10 and be subject to differing interpretations, and without
11 the benefit of testimony from someone who knows
12 something about that exhibit, then you've got the jury
13 and the Court struggling with what that exhibit means,
14 and I argue that that's not the better procedure.

15 MR. McLEROY: Your Honor, the expert
16 witness and technical expert witness are summarizing and
17 basing their opinions on these exhibits. And as far as
18 we're concerned, they would all be fair game for
19 cross-examination by their expert.

20 THE COURT: Well, the -- I'll -- any
21 exhibits that one side wishes to offer or the other side
22 wishes to offer that are not objected to will be offered
23 en masse, regardless of whether they're referred to by a
24 witness or not, so -- unless someone objects on that
25 basis. And I don't interpret your -- your request to be

1 an objection to that.

2 MR. POWERS: We -- we do object to the
3 introduction of large masses of exhibits that no witness
4 would ever discuss. We don't object to the individual
5 exhibits.

6 THE COURT: Well, if you don't object to
7 the individual object -- individual exhibits, then your
8 objection to the manner of admission of the unobjected
9 to exhibits is overruled.

10 MR. POWERS: Understood. Thank you, Your
11 Honor.

12 THE COURT: All right. What's next?

13 MR. CALDWELL: Your Honor, VirnetX has
14 one other issue.

15 At the pretrial conference, I raised with
16 Your Honor that Microsoft has identified the defense
17 of -- that the scope of the Doctrine of Equivalents that
18 VirnetX intends to apply is limited by legal defenses of
19 disclosure, dedication, and all elements rule. And Your
20 Honor invited us to file a motion.

21 THE COURT: Right. I have that.
22 Is that going to be necessary this morning?

23 MR. CALDWELL: I don't think it is. I
24 just wanted -- I didn't want to --

25 THE COURT: Right.

1 MR. CALDWELL: -- speak now or forever
2 hold my peace.

3 THE COURT: That's not going to be
4 referred to during opening statements?

5 MR. POWERS: It will not.

6 THE COURT: Okay. Very well. I'll take
7 that up probably over the noon hour today.

8 Anything further?

9 MR. McLEROY: No, Your Honor.

10 MR. POWERS: Nothing further, Your Honor.

11 THE COURT: All right. Bring the jury
12 in, please.

13 COURT SECURITY OFFICER: All rise for the
14 jury.

15 (Jury in.)

16 THE COURT: Please be seated.

17 All right. Good morning, Ladies of the
18 Jury. Hope that you've had a good weekend and restful
19 and ready for a long week of sitting and listening and
20 learning.

21 So we're going to get started fairly
22 promptly on time this morning. I have some preliminary
23 instructions to give you regarding the law in this case
24 and what you should follow.

25 I will tell you that while you need to

1 listen to these -- and you're going to be provided with
2 notepads in a little bit, and you're invited to take
3 notes if you wish -- it's not entirely necessary that
4 you do so, because all of these instructions will be
5 given to you in much greater detail at the end of the
6 case.

7 But my purpose is to help give you some
8 framework, understanding of the -- of the terminology
9 that's used, of the legal -- the law relating to the
10 various matters that are at trial.

11 And then after I finish those
12 instructions, the attorneys will give you their opening
13 statements. And that's again where they will present
14 for you at that point the evidence that they believe is
15 going to be presented. And they will fit that within
16 the framework of the law I've given you, and they will
17 present to you what they expect the evidence is going to
18 show you during the course of the trial.

19 So that's to give -- this is -- my
20 instructions are to give you an overview of the law and
21 the instructions you're to follow. And their opening
22 statements will give you an overview of what they expect
23 the evidence to be. And then after we finish the
24 opening statements, we'll go straight into the evidence,
25 okay?

1 All right. Well, let me start with the
2 instructions. These will probably take, hopefully, no
3 more than 30, 40 minutes at the most. And I'll have to
4 pause occasionally to wet my whistle, because they are
5 rather lengthy.

6 All right. Ladies of the Jury: You have
7 now been sworn in as the jury to try this case. As the
8 jury, you will decide the disputed questions of fact.
9 As the Judge, I will decide all questions of law and
10 procedure.

11 From time to time during the trial and at
12 the end of the trial, I will instruct you on the rules
13 of law that you must follow in making your decision.
14 Very soon, the lawyers for each side will make what is
15 called an opening statement. Opening statements are
16 intended to assist you in understanding the evidence.
17 However, what the lawyers say during their opening
18 statements is not evidence. The only evidence that you
19 will hear and that you will rely upon in making your
20 decision is what you hear from this witness stand over
21 here or by way of deposition or by way of exhibits that
22 are introduced into evidence.

23 Now, the party who brings the lawsuit is
24 the Plaintiff. In this action, the Plaintiff is
25 VirnetX, Inc., who will be referred to as either the

1 Plaintiff or VirnetX during this trial.

2 The party against whom this suit is
3 brought is called the Defendant. In this action, the
4 Defendant is Microsoft Corporation, who will be referred
5 to as Microsoft or the Defendant during these
6 proceedings.

7 This is a case of alleged patent
8 infringement.

9 After the opening statements, VirnetX
10 will call witnesses and present evidence. Then
11 Microsoft will have an opportunity to call witnesses and
12 present evidence. Then, after all -- you've heard all
13 of the evidence, I will then instruct you on the
14 applicable law. I'll give you detailed instructions
15 both orally as I'm doing now, and at end of the case,
16 you will have those written instructions to take with
17 you to the jury room.

18 After I've given you your final
19 instructions, after all the evidence is in, you've heard
20 the final instructions, then you'll hear the closing
21 argument of the attorneys. After you've heard their
22 closing arguments, then and only then will you retire to
23 the jury room to -- for the first time, start to discuss
24 the case, deliberate and reach a verdict.

25 Now that's a broad overview of what's

1 going to be happening over the next week.

2 During this case, I want you to keep an
3 open mind. Do not decide any fact until you've heard
4 all of the evidence, the closing arguments, and my
5 instructions. Pay close attention to the evidence.

6 If you would like to take notes during
7 the trial, you may do so. The court security officer
8 will now pass out to you notebooks for you to take
9 instructions -- or take notes, if you wish.

10 Inside the notebook, you should find a
11 blank pad. The first thing that I would encourage you
12 to do is to write your name on the first page of the
13 blank pad.

14 Open that notebook and see if there's not
15 a stenographer's pad in there. Is there?

16 Okay. Well, on the first page of that
17 stenographer's pad, when you get it -- or actually on
18 the outside cover, write your name. That will be your
19 notebook for the -- for the course of the trial.

20 There's some other things in that black
21 notebook that I'll go over with you in a moment, but for
22 now, just get your notepad, get your name written on the
23 front cover, and then you can flip over to the second
24 page, and you're welcome to take notes, if you wish.

25 Again, all of these instructions will be

1 repeated to you again later, and they will be provided
2 to you in writing later. But feel free to take any
3 notes you wish.

4 Let me give you some instructions about
5 notes, if you do decide to take them. If you decide to
6 take notes in this case, be careful that you don't get
7 so involved in your note-taking that you become
8 distracted and miss part of the testimony in the case.

9 Your notes are to be used only as aids to
10 your memory. And if your memory should later be
11 different from your notes, you should rely on your
12 memory and not on your notes.

13 Also, don't be unduly influenced by the
14 notes of other jurors. A juror's notes are not entitled
15 to any greater weight than the recollection of each
16 juror concerning the testimony. For example, all
17 because someone has written something down doesn't
18 necessarily mean that they heard it right or that they
19 wrote it down correctly.

20 So just because it's written down doesn't
21 mean that it's to be given any greater weight than just
22 what your memory would be. But it is there to help you.
23 Even though our court reporter here is making
24 stenographic notes of everything that is said, a
25 typewritten copy of the testimony will not -- I

1 repeat -- will not be available for your use during
2 deliberations.

3 On the other hand, any exhibits that are
4 introduced into evidence will be available to you during
5 your deliberations.

6 Until the trial is over, do not discuss
7 this case with anyone and do not permit anyone to
8 discuss this case in your presence. This includes your
9 family and friends.

10 Do not discuss the case even with the
11 other jurors, with your fellow jurors, until all of the
12 jurors are in the jury room at the end of the case, and
13 you actually begin deliberating. So as I told you last
14 week, when you go to lunch or take a break, talk about
15 anything you wish, but don't talk about this case.

16 If anyone should attempt to discuss this
17 case with you or to approach you concerning the case,
18 you should inform me immediately or through my Court
19 staff.

20 During this trial you should hold
21 yourself completely apart from the people involved in
22 the case: The parties, the witnesses, the attorneys,
23 and the persons associated with them. As you can see,
24 there are a lot of people in the courtroom and a lot of
25 attorneys involved in the case.

1 You've got a juror badge on, and I'm
2 instructing everyone in the audience and in the
3 courtroom that they should avoid having any conversation
4 with you or any contact with you. Realize when they
5 don't visit with you and when you don't visit with them,
6 neither one of you are being rude to the other.

7 Just you're a juror; you need to hold
8 yourself apart. Not that you would say anything
9 improper or they would, but not only do we need to be
10 fair, we need to give the appearance of being fair. So
11 be sure that you hold yourself apart.

12 Also, if you have any type of
13 social-networking internet site or tool, like Facebook,
14 MySpace, or Twitter, you should not discuss or even
15 mention the case at all on any of those sites. So no
16 postings on Twitter, no discussion on Facebook, or on
17 any of those social-networking sites.

18 Do not post updates about what is going
19 on in the case. Do not send or receive text messages
20 about the case. That would be entirely improper. And
21 if you were to do that, it can result in all of the time
22 and expense that everybody has spent getting the case to
23 this point, and trying the case can be put in jeopardy.
24 So please follow those instructions very, very
25 carefully.

1 Also, do not make any independent
2 investigation of any fact or matter in this case. Do
3 not learn anything about the case from any outside
4 source. Do not watch TV or read the newspaper, if
5 there's anything in it about this case. Do not use the
6 internet or Google to try to find out more information
7 about the case, the parties, or the attorneys in this
8 case.

9 For example, if you have a computer at
10 home during this case, don't go home and get on your
11 home computer and start trying to figure things out or
12 Google stuff. And the reason for that, again, is very,
13 very important.

14 You are to be guided only by the evidence
15 that you hear -- hear in this courtroom, and any type of
16 independent investigation would be extremely improper
17 and, again, could put these proceedings in jeopardy. So
18 go only by what you see and hear in the courtroom and
19 nothing else. Make no independent investigation.

20 During the trial, it may be necessary for
21 me to confer with the lawyers out of your hearing or to
22 conduct a part of the trial out of your presence. I
23 will handle these matters as briefly and as conveniently
24 for you as I can, but you should remember that they are
25 a necessary part of the trial.

1 And if you have to wait in the jury
2 room -- and, again, I'm going to try to keep that to a
3 real minimum. I'm going to try to deal with anything I
4 need to take up with the attorneys during a break or
5 during the noon hour or after hours or before hours,
6 because I want your time to be spent this week here in
7 the jury box hearing evidence.

8 But those occasions will come up where
9 you're going to be in the jury room, and you're going to
10 be wondering, well, why are we sitting in here? What's
11 going on? Just realize that's part of the case. Again,
12 we will try to hold it to a minimum.

13 Now, let me visit with you about the
14 parties and the nature of this case. As I said, this is
15 a patent case. This case involves two patents
16 identified by their numbers as follows, and this may be
17 where you want to start making some notes, if you wish.

18 The first one is Patent No. 6,502,135,
19 and for simplicity, that's just going to be referred to
20 as the '135 patent. So if I were making notes, I might
21 say, okay, this case involves the '135 patent, and then
22 it also involves the '180 patent. That's Patent No.
23 7,188,180. Again, it's referred to by the last three
24 digits of the patent number.

25 So the case involves two patents: The

1 '135 and the '180.

2 These patents -- these two patents may be
3 referred to from time to time as the patents-in-suit.
4 That means they're the patents that are involved in this
5 lawsuit. These patents generally relate to virtual
6 private networks, and you'll hear a lot more about what
7 a virtual private network is, also sometimes referred to
8 as VPN.

9 You heard some during voir dire
10 examination, but you're going to hear a lot more during
11 the opening statements of the attorneys and during the
12 evidence in the case.

13 All right. In this case, VirnetX, the
14 Plaintiff, contends that Microsoft, the Defendant, is
15 infringing the patents-in-suit, those two patents, the
16 '180 and the '135 patent.

17 And they contend that they are infringing
18 by making, using, selling, offering for sell, or
19 importing Microsoft's accused software products and by
20 causing others to infringe.

21 VirnetX also contends that Microsoft's
22 infringement is willful.

23 Finally, part -- finally, VirnetX
24 contends that it is entitled to damages as a result of
25 Microsoft's infringement.

1 Microsoft, on the other hand, denies that
2 it is infringing, willfully or otherwise, and contends
3 that the patents-in-suit are invalid as being either
4 anticipated by or obvious in light of what is called
5 prior art.

6 Microsoft further contends that the
7 asserted claims of the '135 patent are invalid, because
8 the '135 patent specification does not satisfy the
9 statutory requirements of setting forth an adequate
10 written description or disclosing the inventor's best
11 mode.

12 Now, that may all sound like Greek to you
13 right now. It's a lot of new words thrown at you. I'm
14 going to define a lot of those words for you as I go
15 through the instructions. The attorneys are going to
16 discuss them in their opening statements. The witnesses
17 are going to help you understand those -- those words.
18 So don't feel overwhelmed at this stage. You're going
19 to get a lot of -- lot of education this week and lot of
20 help from the attorneys and from the witnesses for both
21 sides.

22 So let me go back and discuss with you
23 the patent system, generally, the U.S. patent system.
24 You saw some of that on the video that you saw on the
25 first day when you came here. I'm going to go back over

1 some of that with you.

2 Patents are issued by the United States
3 Patent & Trademark Office, which is part of the United
4 States government. The United States government is
5 empowered by the United States Constitution to enact
6 patent laws and issue patents to protect inventions.
7 Inventions that are protected by patents may be of
8 products, compositions, or of methods for doing things
9 and for using or making a product or composition.

10 The purpose of the patent system is to
11 help advance science and technology. The patent system
12 achieves this purpose by granting to the owner of a
13 patent the right, for the life of the patent, to exclude
14 any other person from making, using, offering for sale,
15 or selling anywhere in the United States the invention
16 covered by the patent.

17 A patent has a life for a limited amount
18 of time, which for the patent involved in this case has
19 not yet ended. Once a patent expires, the patent owner
20 may no longer exclude anyone from making use of the
21 invention claimed in the patent.

22 The invention then becomes part of the
23 public domain, which means that anyone is free to use
24 it; that is, after the term of the patent has expired.
25 But during the term of the patent, if another person,

1 without the patent owner's permission, makes, uses,
2 sells, or offers to sell something that is covered by
3 the claims of the patent, then that person is said to
4 have infringed the patent.

5 The patent owner may enforce a patent
6 against other persons or companies believed to be
7 infringers in a lawsuit in federal court as in this
8 case.

9 To be entitled to patent protection, an
10 invention must be new, useful, and non-obvious. As I
11 noted, a patent gives its owner the right to exclude
12 other people from making, using, selling, or offering
13 for sale what is covered by the claims of the patent.

14 Everyone, however, has the right to use
15 existing knowledge and principles. A patent cannot
16 remove from the public the ability of what was known or
17 obvious before the invention was made or patent
18 protection sought.

19 The granting of a patent by the United
20 States Patent & Trademark Office, however, carries with
21 it the presumption that the patent is valid. From the
22 issuance of a patent, it is presumed that its subject
23 matter is new, useful, and constitutes an advance that
24 was not, at the time of the invention was made, obvious
25 to one of ordinary skill in the art.

1 However, that presumption may be rebutted
2 by -- at trial, and you, the finder of fact, may find
3 the patent to be invalid.

4 Now, let's talk about the various parts
5 of a patent.

6 A patent includes two basic parts: A
7 written description of the invention and the patent
8 claims.

9 The written description may include
10 drawings, is often referred to as the specification of
11 the patent.

12 Now, if you will look in the notebook,
13 you will find a copy of the '180 patent. If you would,
14 open your notebook and see if you can locate that.
15 Everybody have it?

16 It should have a tab on it. And then
17 you'll see a page, in the upper left-hand corner, it
18 says United States patent. And then on the right-hand
19 side it says Patent No. U.S. 7,188,180B2. That's the
20 '180 patent.

21 That first page is the cover page of the
22 '180 patent, and it provides identifying information,
23 including the date the patent issued.

24 You see that in the upper right-hand
25 corner -- well, it shows the date of the patent, March

1 6th, 2007. The patent number, along the top, as well at
2 the inventors' names, the filing date.

3 You'll notice over on the left-hand
4 column about halfway down, it says filed November 7th,
5 2003. That's the filing date.

6 The assignee up -- you'll see a little
7 higher up on that left-hand column, there's a No. 73 out
8 beside it. It says assignee, VirnetX, Inc. That's who
9 the patent was assigned to, which is the Plaintiff in
10 this case.

11 You will also see a list of what's called
12 prior art publications considered in the Patent Office
13 when deciding to issue the patent.

14 Now, the specification of the '180 patent
15 begins with an abstract found on the cover page. That's
16 in the lower right-hand corner of the patent on the
17 front page.

18 The abstract is a brief statement about
19 the subject matter of the patent. You'll see it starts
20 with the first sentence: A technique is disclosed for
21 establishing a secure communication link between a first
22 computer and a second computer over a computer network.
23 And then it goes on to give a summary or an abstract of
24 what the inventor is claiming the invention is.

25 Next are drawings, which you will see

1 are -- appear beginning on Page 3. You will see
2 Figure 1. And that continues for the next 37 pages --
3 or it's Figures 1 through 37 on the next 40 pages.

4 I'm not going to ask you to look at all
5 of those, but if you will, flip all the way over to
6 Figure 40, which -- or Figure 37, which is on Page 43 --
7 or Page -- Sheet 40 of 40 of the patent.

8 All right. If you've found Figure 37,
9 turn one more page, and that is the beginning of the
10 written description.

11 Now, the drawings, Figures 1 through 37,
12 those depict various aspects or features of the
13 invention. The drawings are described in words later in
14 the patent description. Beginning on that page after
15 the drawings, that is where the written description of
16 the invention begins.

17 In this portion of the patent, each page
18 is divided into two columns, which are numbered at the
19 top.

20 Is everyone looking at the page that has
21 a 1 over the first column and a 2 over the second
22 column? Everybody have that page?

23 It's the first page following the
24 drawings.

25 So you'll see that's Column 1 and 2. And

1 then you'll see down the middle of the page are some
2 little numbers. There's a 5, a 10, a 15, a 20.

3 You follow those? Everybody see those?

4 Those are the line numbers. So what this
5 allows you to do is, if someone wants to refer you to a
6 particular part of the patent, they may refer you to
7 Column 1, Line -- let me see what would be a good
8 example -- let's say Line 25.

9 So if you look in Column 1 and then you
10 look down in the middle little numbers down to 25, you
11 would be at Column 1, Line 25. And that's where the
12 section entitled, Background of the Invention, lies.
13 And, likewise, you could refer to any column number or
14 any line and follow right in the patent to where it
15 goes.

16 Now, this written description includes a
17 background section, which is on Column 1, Line 25. And
18 then if you'll flip the page over to the next page on
19 Column 3, Line 9, that begins the summary of the
20 invention. And that goes on for several pages over to
21 Column 8.

22 And on Column 8, there's a brief
23 description of the drawings where it discusses what each
24 one of the drawings say. Then over on Column 9 begins a
25 detailed description of the invention down on Column 9,

1 Line 46.

2 Is everybody up with me?

3 Okay. We're making patent experts out of
4 y'all real fast here.

5 In the -- through the detailed
6 description of the invention, it goes through a very
7 detailed description for many pages, and it includes
8 some specific examples within that detailed description.

9 Now, that description goes on until --
10 near the end of the written description is what we call
11 the claims of the patent. And if you'll flip all the
12 way over to -- it's near the end, beginning on
13 Column 56. So turn all the way over to Column 56 in the
14 patent.

15 Everybody have Column 56?

16 Okay. Look down Column 56 to Line 48,
17 and you'll see what it says is, What is Claimed is,
18 colon, and then 1. And 1 begins a method for accessing
19 a secure computer network address comprising steps of,
20 and then it lists several steps.

21 And then you'll see a No. 2. And then on
22 the next page, you'll see on over 3, 4, 5. And it goes
23 on all the way to Column 60, Line 34 where it ends. And
24 as you'll see, there are 41 claims over on Column 60 at
25 the end of the patent. There are 41 claims.

1 Now, all of those claims are not being
2 asserted, just certain ones, and that will be discussed
3 with you in greater detail later. But for now, let's go
4 back to Column 56, Claim 1, which is one of the asserted
5 claims. And I'm going to give you some specific
6 instructions about what a claim means.

7 The claims of a patent are the main focus
8 of a patent case, because the claims are what define the
9 patent owner's rights under the law. That is, the
10 claims define what the patent owner may exclude other --
11 others from doing during the term of the patent.

12 The claims of a patent serve two
13 purposes. First, they set the boundaries of the
14 invention covered by the patent.

15 Second, they provide notice to the public
16 of what those boundaries are. Thus, when a product or a
17 method is accused of infringing a patent, the patent
18 claims are compared to the accused product or method to
19 determine whether there is infringement.

20 The claims of the patent are what are
21 infringed when patent infringement occurs, because the
22 claims define what the patent is.

23 The claims are also at issue when the
24 validity of a patent is challenged. In reaching your
25 determination with respect to infringement and validity,

1 you must consider each claim separately.

2 In your notebook, you are provided with
3 this Court's construction of the meaning of certain
4 terms in the asserted claims in this patent. You must
5 use these meanings that I give to you when you decide
6 the issues of infringement and invalidity.

7 If you'll turn over -- I think it's the
8 next tab in your notebook. You should see a listing of
9 terms that the Court has construed previously.

10 Everybody find that?

11 You don't need to be too concerned with
12 it right now other than to just know it's there.
13 There are certain words within these claims. For
14 example, within Claim 1, there are certain words that at
15 a pretrial proceeding, the attorneys had different
16 arguments over what a particular word meant. And they
17 asked me to construe it, and I have done that, and I've
18 provided you with those definitions.

19 So it's kind of like if you're reading a
20 book and there's a particular word there that maybe you
21 don't quite understand, you would go to a dictionary to
22 look it up. Well, you would go to my claim construction
23 to look up the meaning of those words, and you'll be
24 guided by those meanings.

25 Now, the attorneys will do a good job of

1 explaining all of that when they get into the evidence,
2 but you just need to know for now that those
3 constructions are there and that they relate to these
4 claim terms.

5 So let's look at Claim 1. It goes
6 through several steps there. I don't think I'll read
7 the whole thing at this time -- well, let's read through
8 it. It might be helpful to you.

9 Claim 1, Column 56 said -- says: A
10 method for accessing a secure computer network address
11 comprising steps of, receiving to secure domain name,
12 sending a query message to a secure domain name service.
13 The query message requesting from the secure domain
14 service a secure computer network address corresponding
15 to the secure domain name.

16 Then receiving from the secure domain
17 name service a response message containing the secure
18 computer network address corresponding to the secure
19 domain name and sending an access request message to the
20 secure computer network address using a virtual private
21 network communication link.

22 So those are the steps of the claim. Now
23 you may not understand what all of those mean at this
24 point, but, again, that will be explained to you during
25 the course of opening statements and during the evidence

1 that you hear in the case.

2 But for now, just realize there's
3 Claim 1; it's one of the asserted claims; and it
4 comprises those various steps that I've mentioned to you
5 or I just read to you.

6 Now, let me visit with you about how a
7 patent such as this is obtained. We've gone over the
8 patent, the various parts of it. Let's talk about how
9 someone obtains a patent.

10 The United States Patent & Trademark
11 Office is the agency of our government that examines
12 patent applications and issues patents just like this
13 one.

14 When an applicant for a patent files a
15 patent application with the Patent & Trademark Office,
16 the application is assigned to a Patent Examiner. And
17 you'll remember that from the video you saw the first
18 day.

19 The Patent Examiner in the Patent &
20 Trademark Office then examines that patent application
21 to determine whether the invention described in the
22 patent application meets the requirements of the patent
23 laws for a patentable invention.

24 In examining a patent application, the
25 Patent Examiner makes a search in the Patent Office

1 records for prior art -- and you'll hear that referred
2 to a lot -- for prior art pertinent to the claims of the
3 patent application.

4 The Patent Office records may or may not
5 contain all of the prior art pertinent to the claims of
6 the patent application.

7 The prior art is defined by statute, and
8 I will give specific instructions after the close of the
9 evidence as to what constitutes prior art.

10 But, generally speaking, prior art is
11 technical information and knowledge that was known to
12 the public either before the invention by the applicant
13 or more than a year before the effective date of the
14 application.

15 The Patent Examiner advises the applicant
16 of his or her findings in a communication called an
17 office action. The Examiner may reject the claims, if
18 he or she believes they do not meet the requirements for
19 patentable inventions.

20 The applicant may respond to the
21 rejection with arguments to support the claims and may
22 sometimes make changes or amend the claims or submit new
23 claims.

24 If the Examiner concludes that the legal
25 requirements for a patent have been satisfied, he or she

1 allows the claims, and the application issues as a
2 patent.

3 The process from the filing of the patent
4 application to the issuance of the patent is called
5 patent prosecution. And that's what I've just described
6 to you that goes on between the applicant and the Patent
7 Office.

8 The record of papers relating to that
9 patent prosecution is referred to as the -- as the
10 prosecution history for that patent, or the file
11 history. In other words, it's documents that relate to
12 what transpired between the applicant and the Patent &
13 Trademark Office.

14 So that generally is how the patent
15 process works.

16 Now, let me turn to the issues that you
17 are going to be deciding as the jury in this case. I'm
18 now going to give you some information about those
19 issues that are going to be presented to you at the
20 trial as well as a short overview of the applicable law
21 relating to those.

22 At the close of the trial, you will be
23 given much more specific instructions that you must
24 follow in reaching your verdict. You will also be given
25 a verdict form and questions that you must answer in

1 providing your verdict. That will all transpire at the
2 end of the case.

3 But now let me instruct you on the
4 various instructions that you will follow in deciding
5 the case.

6 First, I want to visit with you about the
7 burdens of proof.

8 In any legal action, facts must be proved
9 by a required standard of evidence known as the burden
10 of proof. You may have heard about this in a criminal
11 case, proof beyond a reasonable doubt; or in a civil
12 case, it's proof beyond -- or proof by a preponderance
13 of the evidence.

14 In a case such as this, there are two
15 different burdens of proof that are used. The first is
16 what's called the preponderance of the evidence
17 standard; and the second is called the clear and
18 convincing evidence standard.

19 The standard beyond a reasonable doubt
20 that's used in criminal cases, that doesn't apply in a
21 civil case like this. We have two standards:
22 Preponderance of the evidence and clear and convincing
23 evidence.

24 In this case, VirnetX must prove its
25 claim of patent infringement by a preponderance of the

1 evidence. When a party has the burden of proof by a
2 preponderance of the evidence, it means that you must be
3 persuaded that what the party seeks to prove is more
4 probably true than not true.

5 To put it another way, if you were to put
6 the evidence for and against the party who must prove
7 the fact on the opposite sides of a scale, a
8 preponderance of the evidence requires that the scale
9 tip at least somewhat toward the party who has the
10 burden of proof. That's the preponderance of the
11 evidence standard.

12 Microsoft has the burden of proving its
13 defense of invalidity by a heavier burden called the
14 clear and convincing evidence standard.

15 When a party has to prove something by
16 clear and convincing evidence, it means that the
17 evidence must produce, in your minds, a firm belief or
18 conviction as to the matter sought to be established.
19 In other words, if you were to put the evidence for and
20 against the party who must prove the fact on the
21 opposite sides of a scale, the clear and convincing
22 evidence standard requires that the scale tip more
23 heavily toward the party who has the burden of proof.

24 Again, you may have heard of a burden of
25 proof used in criminal cases called beyond a reasonable

1 doubt. That burden is the highest burden of proof and
2 is used only in criminal cases. It does not apply to
3 this case. You should, therefore, put that standard,
4 beyond a reasonable doubt, out of your mind for purposes
5 of this case.

6 Now let me visit with you about
7 infringement.

8 As I told you, VirnetX contends that
9 Microsoft infringes Claims 1, 10, and 12 of the '180
10 patent, and Claims 1, 4, 15, 17, 20, 31, 33, and 35 of
11 the '180 patent by making, using, offering for sale,
12 selling, and importing into the United States certain
13 accused products and using certain accused methods.
14 This is called direct infringement.

15 VirnetX also contends that Microsoft
16 infringes indirectly by inducing or contributing to the
17 direct infringement of others.

18 I will first tell you about direct
19 infringement, and then I will tell you about indirect
20 infringement.

21 First, direct infringement. VirnetX
22 seeks to prove direct infringement of the '180 patent by
23 literal infringement. To prove literal infringement of
24 a particular claim, VirnetX must prove by a
25 preponderance of the evidence that the accused products

1 or accused manner of use of the accused products
2 contains each and every limitation of that particular
3 claim.

4 VirnetX also seeks to prove direct
5 infringement of both patents through the Doctrine of
6 Equivalents. The Doctrine of Equivalents provides that
7 patent protection is not limited to a claim's literal
8 terms but also embraces its equivalents.

9 To prove infringement under the Doctrine
10 of Equivalents, VirnetX must prove by a preponderance of
11 the evidence that for each claim limitation not
12 literally met, the limitation is met equivalently in the
13 accused manner of use.

14 I will tell you much more about what is
15 meant by equivalence at the end of the case, but just
16 realize that those are the two ways of infringement:
17 Direct infringement and Doctrine of Equivalents.

18 Now with regard to indirect infringement.
19 VirnetX also alleges that Microsoft has indirectly
20 infringed the asserted claims by inducing and/or
21 contributing to another's direct infringement.

22 To prove that Microsoft induced someone
23 else to infringe, VirnetX must prove by a preponderance
24 of the evidence that Microsoft encouraged or instructed
25 another person to make or use the patented apparatuses

1 or use the patented methods in a manner that infringes,
2 and that Microsoft knew of the patent and knew or should
3 have known that the encouragement or instructions would
4 result in the other person doing that which you find to
5 be an infringement.

6 To prove that Microsoft contributed to
7 another's direct infringement, VirnetX must prove by a
8 preponderance of the evidence that Microsoft sold or
9 supplied to another person a component that is a
10 material part of the patented invention and is not
11 suitable for other substantial non-infringing uses.
12 VirnetX must also prove that the other person directly
13 infringed the patent claims and that Microsoft knew that
14 the component was especially made for use in an
15 infringing manner.

16 Microsoft denies that it has either
17 directly or indirectly infringed any of the claims of
18 the patents-in-suit.

19 Now, with regard to willful infringement.
20 VirnetX also claims that Microsoft willfully infringed
21 the patent claims. To prove willful infringement,
22 VirnetX must prove that Microsoft acted despite an
23 objectively high likelihood that its actions constituted
24 infringement of a valid patent and that Microsoft either
25 knew or should have known of that risk.

1 VirnetX's willful infringement claim
2 requires a higher burden of proof, the clear and
3 convincing standard, than VirnetX's other claims, which
4 require proof by a preponderance of the evidence.

5 I will explain in more detail at the end
6 of the case how you decide whether infringement is
7 willful.

8 Now with regard to invalidity.

9 Microsoft contends that the asserted
10 claims of the patents-in-suit are invalid. Invalidity
11 is a defense to a patent infringement. A person accused
12 of infringement has the right to assert that the claimed
13 invention in a patent did not meet the requirements of
14 patentability and, therefore, that the patent claim is
15 invalid.

16 However, the granting of a patent by the
17 Patent & Trademark Office carries with it the
18 presumption that the patent is valid. The presumption
19 of patent validity imposes the burden on Microsoft to
20 prove invalidity by the clear and convincing evidence
21 standard.

22 I will now explain to you briefly the
23 legal requirements for each of the grounds on which
24 Microsoft relies in its contention that the asserted
25 claims of the patents are invalid.

1 I will provide more details for each
2 ground in my final instructions to you at the end of the
3 case.

4 First is the defense of anticipation.
5 Microsoft contends that the inventions covered by the
6 asserted claims of the patents-in-suit are not new. An
7 invention is not new -- an invention that is not new is
8 said to have been anticipated by the prior art.

9 To prove that a claim is anticipated by
10 the prior art, Microsoft must prove by clear and
11 convincing evidence that each and every limitation of
12 the claim was present in a single item of prior art.

13 Next is obviousness.

14 Microsoft also contends that a number of
15 asserted claims of the patents-in-suit are invalid for
16 obviousness.

17 To prove invalidity of a patent based on
18 obviousness, Microsoft must prove by clear and
19 convincing evidence that the invention defined by the
20 claim would have been obvious to a hypothetical person
21 of ordinary skill in the art at the time the invention
22 was made.

23 It will be up to you to decide the level
24 of ordinary skill in the art of the '135 and the '180
25 patents based on all the evidence introduced at trial,

1 including the level of education and experience of
2 persons working in the field, the type of problems
3 encountered in the field, and the sophistication of the
4 technology.

5 So we've discussed two ways that a patent
6 can be found invalid: Anticipation and/or obviousness.

7 Next is written description.

8 Microsoft also contends that the asserted
9 claims of the '135 patent are invalid, because the
10 description of the invention in the specification does
11 not meet certain requirements.

12 A patent claim is invalid, if the
13 specification of the patent does not contain an adequate
14 written description of the claimed invention. That is
15 referred to as the written description requirement.

16 To succeed, Microsoft must show by clear
17 and convincing evidence that the specification fails to
18 meet the law's requirements for a description of the
19 written invention.

20 I will describe in more detail at the end
21 of the case how you decide the issue of written
22 description.

23 Next is what's called best mode.

24 Microsoft also contends that the asserted
25 claims of the patent are invalid, because the patent

1 does not contain a description of the best way to make,
2 use, and carry out the claimed invention. This is
3 referred to as the best mode requirement.

4 In order to prove that the asserted
5 claims of the patents-in-suit are invalid for failure to
6 disclose the best mode of the invention, Microsoft must
7 prove by clear and convincing evidence that, first, at
8 the time the application was filed, the inventor knew of
9 a best mode of performing the claimed invention; and,
10 second, that the patents-in-suit do not disclose that
11 best mode.

12 I will describe in mere detail at the end
13 of the case how you decide the issue of best mode.

14 Now, that concludes the instructions
15 regarding infringement and the instructions regarding
16 invalidity.

17 Now, let me give you some instructions
18 regarding damages.

19 VirnetX claims that as a result of
20 Microsoft's infringement, it is entitled to damages in
21 the form of a reasonable royalty on each of Microsoft's
22 accused products.

23 Damages cannot be speculative. VirnetX
24 must prove the damages it has suffered as a result of
25 Microsoft's alleged infringement by a preponderance of

1 the evidence.

2 The fact that I am instructing you about
3 damages now does not mean that VirnetX is or is not
4 entitled to recover damages. I will explain to you
5 further at the end of the trial how a reasonable royalty
6 is determined.

7 And at the end of the trial, you will get
8 a written charge that will have all of these
9 instructions in it in much more detail than I am giving
10 them to you now. And you will also have a verdict form
11 that will ask you some very simple questions dealing
12 with the issues of infringement, invalidity, and
13 damages.

14 So that's what you're going to be
15 deciding in this case, is infringement, invalidity, and
16 damages.

17 Now, let me visit with you about the
18 claims of the patent again, more specifically
19 construction of the claims.

20 I will instruct you now and at the end of
21 the case about the meaning of some of the claim
22 language. You must use these meanings I give you when
23 you decide the issues of infringement and invalidity.

24 In deciding whether or not an accused
25 product infringes the patent, the first step is to

1 understand the meaning of the words used in the patent
2 claims. It is my job as Judge to determine what the
3 patent claims mean and to instruct you about that
4 meaning.

5 You must accept the meanings I give you
6 and use them when you decide whether or not a patent
7 claim is infringed and whether or not a patent is
8 invalid.

9 It may be helpful to refer back to the
10 patents in the notebook as I discuss the claims at issue
11 here. The claims are at the end of each patent.

12 In the '135 patent, the claims start with
13 Column 47, Line 20. And in the '180 patent, the claims
14 start with Column 56, Line 48.

15 The patent claims may exist in two forms
16 referred to as independent claims and dependent claims.
17 An independent claim does not refer to any other claim
18 of the patent. It is not necessary to look at any other
19 claim to determine what an independent claim covers.

20 For example, Claim 1 of the '180 patent
21 is an independent claim.

22 And, if you will, turn to Claim 1 of the
23 '180 patent. So find the '180 patent and turn over to
24 Column No. 56. And you'll see down at Column 56,
25 Line 48, it says, What is claimed is Claim 1, a method

1 for accessing a secure computer address comprising steps
2 of, and then it gives the steps.

3 That's what's called an independent
4 claim. It's not dependent on any other claim.

5 But a dependent claim is one that refers
6 to at least one other claim in the patent. A dependent
7 claim includes each of the limitations of the other
8 claim or claims to which it refers as well as the
9 additional limitations recited in the dependent claim.

10 Therefore, to determine what a dependent
11 claim covers, it is necessary to look at both the
12 dependent claim and the other claim or claims to which
13 it refers.

14 For example, Claim 4 of the '180
15 patent -- if you'll turn over to the next page,
16 Column 57, Line 7, you'll see the No. 4. That's
17 Claim 4.

18 And Claim 4 says: The method, according
19 to Claim 1. So right there, it's incorporated in
20 Claim 1 and all of its elements into this, but then it
21 has the additional element. It says: The method
22 according to Claim 1 wherein the response message
23 contains provision -- provisioning information for the
24 virtual private network.

25 So Claim 4 is what we call a dependent

1 claim.

2 The claims of the patents-in-suit use the
3 word -- use the words comprises and comprising. For
4 example, back to Claim 1, you see at the beginning of
5 Claim 1, it says a method for accessing a secure
6 computer network address comprising steps of.

7 Now, a claim that uses the words
8 comprising or comprises means including or containing.
9 A claim that uses the word comprising or comprises is
10 not limited to products or methods having only the
11 elements that are recited in the claim, but also covers
12 products or methods that add additional elements.

13 Take, for example, a claim that covers a
14 table. If the claim recites a table comprising a table
15 top, legs, and glue, the claim will cover any table that
16 contains these structures -- structures, even if the
17 table also contains other structures, such as a leaf or
18 wheels on the legs. That's a very simple example of
19 what using the word comprising means. In other words,
20 it can have other features in addition to those that are
21 covered by the patent.

22 I have now instructed you as to the types
23 of claims at issue in this case. I am next going to
24 define the meaning of words used in the patent claims at
25 issue -- issues. You must use the definitions I provide

1 to you when you decide infringement and invalidity.
2 If you'll now take a look at the chart at the back of
3 your book, you will see the various instructions that I
4 have given to you. There's not very many of them; it's
5 all on one page.

6 You will see, for example, up at the top
7 under the '135 network -- or '135 patent, virtual
8 private network, or VPN.

9 Does everybody have that?

10 It should be the last tab in your
11 notebook. It has a sheet that looks like this
12 (indicates).

13 A JUROR: First page?

14 THE COURT: First page of your notebook.
15 Okay. Sorry about that. First page OF your notebook.
16 I don't believe it has a title on the page, but it has
17 '135 patent and '180 patent in the middle.

18 Everybody have it?

19 Okay. You'll see at the first one,
20 virtual private network. The Court has -- the parties
21 came to me and said we need you to define what this
22 means, and they presented various arguments. And this
23 is the construction that I determined, and it's the
24 construction that you will follow in trying this case.

25 A virtual private network, or VPN, is a

1 network of computers which privately communicate with
2 communication paths between the computers.

3 So that's an example of a definition.
4 I'm not going to go through all of these now. They're
5 there for your reference, and you can -- you'll hear
6 about them during the case, but you'll see the various
7 words that have been defined and construed by the Court
8 with regard to the claims.

9 All of this will become clear to you as
10 the trial progresses, but this is a good starting place
11 for you to help you understand some of the basic
12 elements of a patent and some of the basic language and
13 nomenclature.

14 Again, if you're feeling a little
15 overwhelmed at this point, rest assured there's going to
16 be lots of explanation and lots of time to digest. This
17 is the first time you've heard a lot of these words, a
18 lot of these concepts. You're going to be hearing a lot
19 more about them during the opening statements, during
20 the evidence.

21 We'll have experts from both sides that
22 are going to help you understand this case. And at the
23 end, you'll hear closing arguments. You'll have my
24 Court instructions, and you'll -- you'll be
25 well-equipped to decide this case by the time you get to

1 the end of it.

2 Now, finally, let me just discuss with
3 you your duties as jurors.

4 You have two duties as jurors. Your
5 first duty is to decide the facts from the evidence in
6 the case. That is your job and yours alone.

7 Your second duty is to apply the law that
8 I give you to the facts. You must follow these
9 instructions, even if you disagree with them. Each of
10 the instructions is important, and you must follow all
11 of them.

12 You must perform your duties fairly and
13 impartially.

14 Do not allow sympathy, prejudice, fear,
15 or public opinion to influence you. Nothing I say now
16 and nothing I say or do during the trial is meant to
17 indicate any opinion on my part about what the facts are
18 or about what your verdict should be.

19 You are the sole judges of the facts, and
20 that is your job alone.

21 That concludes my opening instructions to
22 you. It took just a little bit over an hour. We're
23 going to hear opening statements by both sides in a
24 moment.

25 I believe I've given y'all how long?

1 MR. CAWLEY: 45 minutes, Your Honor.

2 THE COURT: All right. Each side is
3 going to have 45 minutes for opening statements. So
4 before we begin, I think we'll take our morning break at
5 this time, give you a chance to have a cup of coffee.
6 We should have some refreshments in there for you. Use
7 the restroom.

8 When we come back, you'll hear opening
9 statements from both sides. That should take about an
10 hour and a half. So if you'll be back here at 10:30,
11 which is 20 minutes from now, we'll begin opening
12 statements.

13 We should be through by noon. Then we'll
14 let you go to lunch, and then we'll come back and start
15 the evidence after lunch.

16 So be in recess until 10:30.

17 COURT SECURITY OFFICER: All rise.

18 THE COURT: Please remember my
19 instructions. Don't discuss the case during your break.

20 (Recess.)

21 COURT SECURITY OFFICER: All rise.

22 (Jury in.)

23 THE COURT: Please be seated.

24 All right. Ladies of the Jury, we will
25 now hear opening statements, first by counsel for the

1 Plaintiff.

2 MR. CAWLEY: Thank you, Your Honor.
3 Ladies of the Jury, every lawsuit is a story, and this
4 one is no exception.

5 The case that you'll hear this week is a
6 story about a small team of people who invented a way to
7 make it easy to communicate safely over the internet.

8 Now, people who actually use computers
9 themselves certainly would be helped by that invention.
10 But as you'll hear this week, the use of computers has
11 become so widespread in our world today, that all of us,
12 whether we actually put our hands on a computer or not,
13 are helped by keeping communications over the internet
14 safe and protected.

15 I'd like to introduce you, again, to the
16 man who led that small team of people.

17 Would you stand up, please, Mr. Munger?

18 This is Mr. Edmund Colby Munger. He goes
19 by the name of Gif, and since he led that team of
20 inventors, I want to tell you a little bit about his
21 story that you'll hear during this trial.

22 You'll hear that Mr. Munger -- if we
23 could dim the lights a little bit -- chose and had an
24 opportunity to attend the United States Naval Academy
25 where he graduated in 1967. He was immediately assigned

1 to duty on a ship off the coast of Vietnam during the
2 Vietnam War.

3 You'll hear that Mr. Munger became the
4 commander of his own ship at the age of only 28 years
5 old; that he spent the next 20 years -- actually, a
6 total of 20 years as an officer in the United States
7 Navy.

8 Now, the reason that that's important for
9 this case and the story that you'll hear in this case is
10 that if you don't know already, you'll learn a little
11 bit about the fact that the United States Navy is
12 heavily dependent on technology: Radar, computers, and
13 things of that nature; and that Mr. Munger, while he was
14 in the Navy, was typically responsible for high-tech
15 matters relating to the ships that he served on.

16 After he retired from the Navy in his
17 early 40s, Mr. Munger joined an unusual company that
18 you'll hear a little bit about in this case. It's
19 called Science Applications International Corporation.
20 Now you may never have heard of that company. It's not
21 well-known.

22 It's unusual, because it's a company that
23 was founded by a nuclear scientist, and his idea for a
24 business was to use private enterprise to provide
25 scientific solutions for problems that the military and

1 other branches of the United States government might
2 have.

3 You'll hear that Mr. Munger was excited
4 to join this company, because he had a lot of respect
5 for the scientists in this company, which is usually
6 called SAIC, that he had worked for or worked with when
7 he was still an officer in the United States Navy.

8 One of the first projects that Mr. Munger
9 worked on at SAIC actually formed a pathway that would
10 eventually lead to the invention in this case.

11 You may remember that during the first
12 Iraq war -- that's the war that President -- the first
13 President Bush invaded Iraq -- that during the first
14 Iraq war, we heard a lot of news accounts about
15 something called scud missiles. You may remember that.

16 Scud missiles were missiles mounted on
17 trucks that the Iraqi army had, that they could put in
18 hiding, under a bridge or elsewhere, then bring out and
19 fire off with no more than a few minutes' notice.

20 You'll hear that the American military
21 did not have an effective way to defend against scuds,
22 and they turned to SAIC and to Mr. Munger to try and
23 find a solution to that problem.

24 What they came up with was a system that
25 came to be known as the Global Hawk. The Global Hawk is

1 an unmanned aircraft that flies very high above the
2 Earth for long periods of time. It had the ability to
3 sense or to see the scud missile launcher on the ground
4 and to communicate actual pictures of that to a
5 satellite orbiting over the Earth.

6 That satellite then had the ability to
7 send those same pictures to a soldier on the ground who
8 would see pictures of the scud, understand where it is,
9 and communicate that information to either aircraft or
10 troops that could attack the scud -- scud missile before
11 it had an opportunity to launch.

12 You'll hear, though, that there was
13 something very unusual about this project. Because time
14 was short, the system had to use a satellite that was a
15 public satellite. It wasn't owned by the military. It
16 was a satellite that any company can rent time on to
17 transmit television pictures or other things.

18 And that presented a grave problem of
19 securing it, because it was possible that someone on the
20 ground -- we'll call them a hacker -- could intercept
21 the communication from the satellite back to the ground,
22 and understand what the military was about to do.

23 Therefore, you will hear Mr. Munger
24 explain that an important part of this Global Hawk
25 program, which he headed, was to secure or find a way to

1 lock up those communications so that a hacker, if they
2 attempted to intercept them, would be locked out and
3 couldn't see the data that was being transmitted from
4 the satellite.

5 This experience in Global Hawk caused
6 Mr. Munger -- you will hear him testify -- to begin
7 thinking about the future of military needs and the
8 future of the need for communication security.

9 You will hear that he wrote a paper,
10 which was read in Washington, D.C., called the Aladdin
11 Paper, and the reason he named it Aladdin was he saw a
12 future in which by rubbing something like a magic lamp,
13 the military and other security agencies would be able
14 to call out all kinds of resources, like satellite
15 communication, like cell phone communication, and like
16 communication over the internet.

17 Mr. Munger's thinking about this issue,
18 and to some extent the Aladdin Paper that was read by
19 people in the military and security agencies, caused a
20 contract to come about between Mr. Munger's company that
21 he worked for, SAIC, and an unusual company called
22 N-Q-Tel.

23 N-Q-Tel was founded by Congress. It was
24 a company set up by Congress. And its purpose was
25 rather than to spend lots of money inside the government

1 developing solutions for the Central Intelligence
2 Agency, that N-Q-Tel would invest relatively small
3 amounts of money with private enterprise so they could
4 come up with better solutions for the things the CIA
5 needed.

6 In return for this, the company would get
7 to keep any inventions that they made along the way.
8 And, of course, the CIA would be able to use those
9 inventions for whatever purpose they needed.

10 There was a particular need that the CIA
11 had that related to this contract between N-Q-Tel and
12 SAIC. And it was that CIA agents, I guess people like
13 spies, but others, might be anywhere in the world and
14 needed to be able to communicate securely back to the
15 CIA. They needed to be able to use the internet to do
16 that.

17 But as you'll learn in this case, the
18 internet is not secure. Therefore, that wouldn't be
19 good enough for the CIA.

20 And the CIA asked Mr. Munger and this
21 company, SAIC, to come up with a solution of how they
22 could communicate securely over the internet.

23 Mr. Munger worked with several other
24 scientists who were on this team and who are also
25 inventors on the patents. One of them is Dr. Bob Short.

1 Dr. Short, if you would stand up, please.

2 Dr. Short is also an inventor, along with
3 his co-worker, Mr. Munger. They still work together to
4 this very day. And you will hear him testify in this
5 case.

6 Thank you, Dr. Short.

7 You will hear him testify how, when SAIC
8 undertook this job for N-Q-Tel and the CIA, he and his
9 team went out and researched different ways that already
10 existed to make communications secure on the internet,
11 because there were some ways that people were already
12 doing it.

13 He and his team of experts were already
14 aware of them, but they did a lot of research and bought
15 a lot of projects -- products to see what was available
16 at that time to see if it would be suitable for what the
17 CIA needed.

18 One that was the most interesting and the
19 one that you'll be hearing about in this case -- in
20 fact, Judge Davis warned you that we'd be talking a lot
21 about this, and now we're about to -- is called a
22 virtual private network.

23 Now because you'll be hearing a lot about
24 virtual private networks in this case, I'd like to
25 interrupt the story of Mr. Munger and his team of

1 inventors working for the CIA for just a minute, so we
2 can spend just a few minutes talking about what this
3 thing called a virtual private network is and what it
4 does.

5 First of all, as you probably already
6 know this, rather than say the mouthful of virtual
7 private network every time, it's frequently abbreviated,
8 VPN. So if you see references or hear references in
9 this to a VPN, you know we're talking about a virtual
10 private network.

11 Now, we'll certainly attempt to keep
12 abbreviations like this to a minimum, because I know it
13 gets confusing very fast. But VPN is one that you're
14 bound to hear.

15 To understand what this VPN, or virtual
16 private network, is, let's talk first about a network.
17 Now that's a word that we use occasionally. It sounds
18 like a net, like a hair net or a fishing net.

19 Frequently, we talk about a network of
20 co-workers, a network of friends, which, in that
21 context, means many communications among people. But
22 here, of course, we're talking about computers and
23 computer networks.

24 If you have a number of computers, they
25 can be connected either with wires or with radio

1 communication or in other ways. And the software on one
2 computer can share information with software on another
3 computer that it's connected to. That's a network.

4 The information could be words, like in
5 an e-mail. The information could be a picture that's
6 sent from one computer to another. The information can
7 be a lot of different things. But the function of the
8 computer network is to allow computers to share
9 information.

10 We have huge computer networks in the
11 world now. This just shows the United States, and it's
12 very much an under-exaggeration of how many computers
13 are on the network in the United States that's known as
14 the internet. All the internet is, is a vast network of
15 computers both in the United States and around the globe
16 that are all linked together.

17 Because they are linked together in this
18 example, someone from Company A who wants to send data
19 or information to Company B can set up a link or a
20 communication over the network. And one of the beauties
21 of the network is that if for some reason that
22 particular path doesn't work, then they can choose this
23 one, a different path, or many other different paths
24 depending on what's available and what's the most
25 efficient.

1 So that's what the network word in a
2 virtual private network is.

3 Private refers to a network that somebody
4 owns and controls all of. They own the computers; they
5 own the wires.

6 If you work in a small business and your
7 business has a network and it owns the computers and it
8 owns the wires that connect them, it's a private
9 network. Nobody out in the public is allowed to use it.
10 A virtual private network -- virtual is a word that
11 we've been hearing a lot in the last few years, and I'm
12 sure you recognize that in this context what it usually
13 means is it's not real; it's not a real, concrete thing
14 that you can touch, but it's something that behaves as
15 if it were real.

16 So a virtual private network is a
17 computer network that's not really private. It goes
18 over publicly available stuff like the internet, but it
19 behaves as though it is private.

20 Now, how would that work?

21 Here we see Company A again, and this
22 time a remote user -- maybe that's an employee of
23 Company A, who's traveling. Looks like he's in Florida
24 or thereabouts, and he wants to communicate securely
25 back to Company A.

1 His computer can set up this connection
2 over the internet. And by using certain techniques that
3 I will tell you a little bit more about in a minute,
4 those connections can be secured.

5 Looks familiar. Looks a lot like the
6 Global Hawk problem and the security between the
7 satellite and the ground. But here it's the path along
8 the internet that's being secured.

9 And once it's secured, a hacker, who
10 attempts to intercept the information, is locked out.
11 They can't see anything useful.

12 This is an example of a virtual private
13 network. It's not actually private, because the remote
14 user in Company A don't own the internet that they're
15 talking over. But we call it a virtual private network,
16 because it behaves as if it were private, and it is as
17 secure as if someone actually owned all the computers
18 and all the wires.

19 This kind of technology existed at the
20 time when Dr. Bob Short and Gif Munger and their team of
21 inventors was trying to find a way to help the CIA
22 communicate securely over the internet.

23 But virtual private networks that you've
24 seen here had a major drawback that made them
25 unacceptable for what the CIA needed and unacceptable

1 for almost all people who needed to communicate securely
2 over the internet.

3 Here's an article from a publication
4 called Network World from 1998, about the time that
5 Dr. Short and Gif Munger were working on this problem.
6 And it says that remote access, which is what we're
7 talking here, is a nightmare for support desks.

8 Staffers never know what combination of
9 CPU modem, operating system, and software configuration
10 they're going to have to support. Adding VPN software
11 makes it worse.

12 Let me show you a document that you'll
13 hear about in the case. This is Plaintiff's
14 Exhibit 983.

15 This is basically an instruction manual
16 for some Microsoft software that was available in the
17 year 2000 that could be used to set up a virtual private
18 network. Let me give you just a sense of what you had
19 to do to set up that virtual private network.

20 First of all, you had to create something
21 called an IPSEC policy, and there were seven -- excuse
22 me -- five steps you had to go through described in the
23 document to do that. But then you had to build a filter
24 list from Net A to Net B, and there were nine steps you
25 had to go through to do that.

1 Then you had to build a filter list from
2 Net A -- Net B to Net A, and there were seven steps you
3 had to do to do that.

4 Then you had to configure a rule for
5 Net A to a Net B tunnel. There were ten steps that you
6 had to follow to do that.

7 Then you had to configure a rule for
8 Net B to Net A. That was seven more steps to do that.
9 That process was so complicated that even experts who
10 were setting this up were encouraged to print out a long
11 list of descriptions of what they had done and get on
12 the phone to try and figure out why their virtual
13 private network wouldn't work.

14 You will hear from Dr. Short and others
15 that the virtual private network software and hardware
16 that was available in the late '90s was too complicated,
17 too cumbersome, and took too long for most people to
18 actually use.

19 You'll also hear that people who worked
20 in the security field know that if security is too
21 complicated for people to use, they just won't use it.

22 If you have a burglar alarm system and
23 the keypad is so complicated that you can't really
24 figure it out, then you're going to leave the house
25 without setting it. That's the way -- that's the way we

1 all are.

2 And the people working on this knew that
3 wasn't a solution for what the CIA needed for one of its
4 agents to be able to quickly but securely communicate
5 over the internet.

6 That then lays the foundation for the
7 invention in this case. You will hear that Mr. Gif
8 Munger, Dr. Short, and two of their colleagues worked on
9 this problem for months. They consulted with other
10 people; they did research. They had to find a solution.
11 How can a VPN be set up quickly and easily?

12 Finally, you'll hear about a train ride
13 that they took coming back from a meeting in New York
14 back to near where they live, in Washington, D.C., in
15 September of 2009.

16 On that train ride, Dr. Short, who you
17 just met, had a breakthrough that would solve the
18 problem of how people can set up VPNs easily.

19 Here at a high level is their invention.
20 Now, of course, you'll hear a lot more about this later
21 on, but in the time that I have right now, let me
22 explain to you that, once again, we have a remote user
23 traveling in Florida, who wants to communicate back to
24 her company. Looks like they're in California.

25 By typing in what's called a domain name,

1 the remote user's computer will trigger something called
2 a DNS request.

3 Now, let me stop there. Those of you who
4 actually used the internet, or have seen it at all, have
5 used a domain name, although you may not have called it
6 that.

7 A domain name simply means the name of
8 something you're trying to reach out to on the internet,
9 such as Amazon.com; that's a domain name; eBay.com;
10 that's a domain name.

11 So a remote user types in the domain name
12 and does one click on her computer. That DNS request
13 then goes to some VPN software that's part of the
14 invention, which sends back information to her computer
15 necessary to set up a connection, not yet a secure
16 connection.

17 There's also software involved in the
18 invention on the far end of the network, this time at
19 Company A. And that software between the two computers
20 automatically negotiates the secure VPN connection
21 between them.

22 And just like we saw before, once that
23 VPN is set up, a hacker is locked out from being able to
24 hack in to information that's traveling on that network.
25 The important thing to remember here is this remote user

1 in Florida didn't have to go through all these steps
2 that I described to you to set up a secure VPN.

3 What she had to do was one click on her
4 computer.

5 Now, Ladies and Gentlemen, you'll hear
6 evidence that this invention solved the problem of VPNs
7 and made them practical solutions to secure
8 communications over the internet.

9 Now, it may be important for you to
10 understand when these events occurred, so let me stop
11 the story again, and let's look at this timeline a
12 moment.

13 We go from 1998 to 2007. It was in 1998
14 that Gif Munger and Bob Short and their co-inventors
15 were working on the Global Hawk program and first
16 encountered this problem of the need to secure
17 communications that were going over public things, like
18 satellites, or later, the internet.

19 It was in 1999 that they thought of the
20 invention in this case which provided a way to make
21 setting up VPNs on the internet easy and practical.

22 In the year 2000, they filed two patent
23 applications for their invention. The first was filed
24 early in the year. And after two years of
25 consideration -- that application was in the United

1 States Patent Office for two years, and after those two
2 years, the Patent Office issued this patent for the
3 invention, agreeing that it was something new and useful
4 and important.

5 The second application that they had
6 filed stayed in the Patent Office for almost seven
7 years, the Patent Office considering it all that time.
8 But at the end of those seven years, the Patent Office
9 issued the second patent in this case; again, finding,
10 as a result of their work, that this invention was
11 something new, something valuable, and something
12 important.

13 Now, we've been talking so far about the
14 VirnetX side of the story. VirnetX is a company that
15 Mr. Munger will explain to you was formed in order to
16 try and make a business out of this invention, and to
17 enforce the patent so that they could receive fair value
18 from anyone who wanted to use the invention.

19 I've been telling you about Mr. Munger,
20 about his team, and about VirnetX, but now let's change
21 the subject a little bit, and I want to talk to you for
22 a few minutes about Microsoft, the Defendant in this
23 case.

24 Microsoft, as you know, is the largest
25 computer software company in the world. Let's take a

1 look at what Microsoft was doing and thinking at the
2 time Mr. Munger and his team had their invention in
3 1999, about the subject of security, and particularly
4 about virtual private networks.

5 Fortunately, we don't have to guess or
6 speculate about what Microsoft was doing, because there
7 have been a lot of documents produced in this case, so
8 we'll have an opportunity to show you some documents
9 that will actually reveal to you what Microsoft was
10 doing.

11 You'll see that in that year, when the
12 inventors had their idea in 1999, Microsoft had this
13 confidential business plan talking about their strategy
14 of how they would win in the marketplace. And they
15 decided that what they needed was to have the best
16 integrated, transparent, which means automatic,
17 policy-based VPN. They recognized they needed an
18 automatic VPN.

19 And that this would help establish
20 Microsoft as a valued leader in security products.
21 In that same document, you'll see that Microsoft
22 recognized that what they needed was transparent
23 end-to-end security, an automatic VPN, just like you
24 heard that the inventors were thinking about and found a
25 way to do.

1 But you'll see that Microsoft, at this
2 time at least, didn't see that way to do it. Other
3 Microsoft documents tell us in this confidential
4 document on the subject of transparent connectivity,
5 which, as you saw in the earlier document, is just a way
6 of saying how can we get all this set up without having
7 to go through all these steps.

8 They said a hard problem is automatic
9 access and configuration. Microsoft recognized that the
10 same problem that Mr. Munger and his co-inventors were
11 working on wasn't something easy to solve. It wasn't
12 something that was obvious. It was a hard problem.

13 But as the next couple of years went by,
14 Microsoft came under increasing pressure to increase the
15 quality of the security products that it was offering to
16 the public.

17 You are probably all familiar with
18 Mr. Bill Gates, who, at the time, was the Chairman of
19 Microsoft, and now the former Chairman.

20 In 2002, he wrote that, we, Microsoft,
21 are now making security improvements an even higher
22 priority than adding features. In other words, instead
23 of coming up with new things the computer could do,
24 Microsoft had now made it an even higher priority to
25 make security improvements.

1 In the next year, Mr. Gates wrote: As we
2 increasingly rely on the internet to communicate and
3 conduct business, a secure computing platform has never
4 been more important. Along with the vast benefits of
5 increased connectivity, new security risks have emerged
6 on the scale that few in our industry fully anticipated.
7 As a leader in the computing industry, Microsoft has a
8 responsibility to help its customers address these
9 concerns so they no longer have to choose between
10 security and usability.

11 Exactly the issue we talked about a
12 minute ago. The keypad on the burglar alarm is too
13 complicated to use. Here Mr. Gates is telling us, in
14 2003, that Microsoft is struggling to find a way so that
15 its customers have something simple enough to use that
16 they don't have to make that choice.

17 In the next year, 2004, Mr. Gates is
18 still very much concerned with security, as is
19 Microsoft. He says that security advancements outlined
20 today, as well as industry collaboration and innovations
21 in security technology for the future, will play a key
22 role in providing users with a safer and more seamless
23 computing experience.

24 In a 19 -- excuse me -- 2004, again, he
25 says, if you look at our resources -- that's Microsoft

1 he's referring to -- and what's the biggest part of that
2 research and development in investment at Microsoft
3 right now, it's focused on security.

4 As a result of this intense focus,
5 Microsoft also recognized one of the key issues they had
6 to solve was security for remote access, just like we
7 saw with the woman in Florida who needed a VPN.

8 In this document in 2004, Microsoft said
9 that enhancing the security of corporate assets
10 worldwide is a top priority for the Microsoft
11 information technology organization.

12 A major concern is remote access -- just
13 what we saw before -- the services and connections that
14 allow approved employees to connect to a corporation's
15 network from a remote location.

16 As a result of these concerns, Microsoft
17 released some products that allowed its customers to
18 connect to virtual private networks very easily. And
19 one that we'll talk about in this case was called Live
20 Communications Server 2005 that was introduced to the
21 market, as you might guess, in 2005.

22 In the literature describing that
23 Microsoft Live Communication Server 2005, Microsoft said
24 that with Live Communication, your team can connect with
25 co-workers, partners, suppliers, and customers in

1 real-time, share critical and time-sensitive
2 information, and collaborate with other organizations as
3 easily as they do today with co-workers, while taking
4 advantage of built-in security measures to help
5 safeguard your proprietary business information.

6 And in another Microsoft document, this
7 time in 2007, in talking about their communications
8 software, Microsoft says: Not only are we able to
9 launch new business communications with just one click,
10 but user set-up and administration is extremely simple.
11 Does that sound familiar?

12 It should, because what you will hear
13 from the testimony in this case by experts highly
14 qualified in this field is that just one click that
15 Microsoft refers to starts the invention that is the
16 same as what was patented by Mr. Munger and Dr. Short
17 and their co-inventors.

18 You'll also see Microsoft documents that
19 establish that this kind of business, this communication
20 software business, was enormously promising for
21 Microsoft financially. You will see that at this time
22 in 2007, they projected that this market was worth an
23 estimated \$45 billion.

24 When Mr. Munger testifies later today,
25 you will hear him explain that during the course of

1 trying to make something of his invention, trying to get
2 people interested in it, trying to make it usable, he
3 was asked to do some research on this Microsoft Live
4 Communication 2005 product, where he began to suspect
5 for the first time that Microsoft was infringing his
6 patents.

7 He told the people at his employer at
8 that time, SAIC, and some other people, and they sent a
9 letter to Microsoft, and that letter said we'd like to
10 contact you in the next week or so to discuss the
11 possibility of offering a license to our '135 patent.

12 We believe the '135 patent would be of
13 interest to your company in connection with this Live
14 Communication Server 2005 product and in connection with
15 Microsoft Office Communicator 2005 product.

16 And the parties exchange some letters
17 back and forth about that possibility. So what you will
18 hear in this case, Ladies and Gentlemen, is that at the
19 end of the day, Microsoft has refused to pay fair value
20 for their use of the patents and the inventions in this
21 case.

22 As a result, Mr. Munger, Mr. Short, and
23 their new company, VirnetX, have been required to file
24 this lawsuit to ask you to award them a reasonable
25 royalty for Microsoft's use of their invention.

1 Now, how much would be a reasonable
2 royalty?

3 Well, you saw that document in which
4 Microsoft projected that the market might be \$45
5 billion. In fact, they were a little pessimistic. You
6 will hear that from its sale of products that use the
7 inventions in this case, Microsoft has made \$48 billion.
8 You will also hear something else interesting. You will
9 hear that back in 2002, SAIC, Mr. Munger's company,
10 entered into a license agreement with a company called
11 SafeNet to use the invention. And you'll hear that at
12 that time SafeNet agreed to pay 20 percent of its
13 revenues from the invention as a reasonable royalty.

14 Now, you'll also hear that SafeNet, under
15 this agreement, was going to be required to spend money
16 to develop the invention so that it would be ready for
17 sale. And a few months after entering this agreement,
18 they decided that they didn't want to spend the money to
19 develop the invention. Therefore, they terminated this
20 agreement.

21 But I believe you'll find, when you hear
22 the evidence, that this agreement entered into my
23 SafeNet and their agreement, at least in the initial
24 negotiation, to pay 20 percent of the revenues is a
25 powerful indicator to you of how valuable this invention

1 really is to people like Microsoft.

2 But VirnetX and Mr. Munger and Mr. Short
3 are not going to ask you to award them anything like 20
4 percent of Microsoft's revenues from the sale of these
5 products.

6 We're going to introduce you later on in
7 the trial, probably on Wednesday, to a man named Brett
8 Reed.

9 If you'd stand up, Mr. Reed.

10 Mr. Reed has been in the business for
11 many, many years of valuating the value of things like
12 patents and the amount of a reasonable royalty.

13 Thank you, Mr. Reed.

14 He'll take you through a lengthy analysis
15 of how professionals in the field do that. Judge Davis
16 will give you some instructions later on in the trial
17 that you'll hear that Mr. Reed followed in doing that.
18 And you'll hear what he concluded is that the \$48
19 billion in Microsoft's revenue from sale of these
20 products should actually be reduced to no more than \$30
21 billion. And he'll explain to you that he's concluded
22 that a lot of that royalty base doesn't have anything to
23 do with the invention and, therefore, he excluded it.

24 Out of what's left of the 30 billion, he
25 has concluded that not the SafeNet's 20 percent is fair,

1 but a fair royalty in this case is less than 1 percent
2 of Microsoft's revenues for the '135 patent and less
3 than 1 percent for the '180 patent.

4 In short, he will tell you that if you
5 take the dollar that Microsoft made from using the
6 invention that a reasonable royalty is one-third of a
7 penny to two-thirds of a penny for each patent.

8 Now, I did refer to pennies, but, of
9 course, we're not talking about pennies here. We're
10 talking about billions. Mr. Reed will show you his
11 calculations and will tell you that applying this
12 approach means that the total reasonable royalty he
13 concludes would be paid by Microsoft to VirnetX is \$242
14 million.

15 That's a lot of money; \$242 million is a
16 lot of money in any context. But, remember, Microsoft,
17 you will hear evidence show you, made an enormous amount
18 of money from the use of this invention.

19 VirnetX asks you only to award them what
20 you find is a reasonable royalty.

21 Now, that's almost the end of my remarks
22 to you this morning before you hear the evidence. But
23 you will also, of course, hear from Microsoft in this
24 case, as you should.

25 But I think that once you've heard all

1 the evidence, you will find that there is a clear path
2 in the evidence which suggests to you that VirnetX
3 should be awarded a reasonable royalty. And I'm afraid
4 that you'll hear that Microsoft in this case will
5 consistently try to distract you and misdirect you from
6 that path.

7 I think that they will argue to you,
8 well, we don't really use the patent. We don't
9 infringe.

10 Well, Ladies and Gentlemen, I would like
11 to introduce you to Dr. Mark Jones. Mark Jones is a
12 professor of computer science at Virginia Tech
13 University.

14 You will hear that in order to really
15 find out whether or not Microsoft infringes, you have to
16 be able to look at Microsoft's secret computer code.
17 And they won't show that to just anybody and show it to
18 the public. Ordinarily, people can't see Microsoft's
19 secret computer code.

20 But you will hear that in this case,
21 Judge Davis has allowed Professor Jones to study that
22 Microsoft code, and he will explain to you after many,
23 many hours of study, his conclusion that Microsoft uses
24 the inventions and infringes the patents.

25 I'll warn you, he'll tell you that

1 conclusion, but then we're going to have to let him
2 spend about two hours, probably on Wednesday, dotting
3 all the Is and crossing all the Ts so that it's entirely
4 clear to you that Microsoft, in fact, does infringe.

5 I think, though, that if Microsoft is not
6 able to distract you by arguing that they don't
7 infringe, the next thing they may say is, well, if we do
8 infringe, it's not willful.

9 Well, remember, Microsoft got that letter
10 in 2006 telling them about the patent. I think you'll
11 hear that they didn't do anything to avoid infringing;
12 that they didn't have any good excuse for believing that
13 they didn't infringe; and that they basically just
14 adopted a head-in-the-sand policy of being indifferent
15 about the patents.

16 Microsoft will then tell you, I believe,
17 well, if you don't buy that we don't infringe and you
18 don't buy that our infringement wasn't willful, how
19 about this: The patent is invalid. Maybe you'll buy
20 that.

21 Ladies and Gentlemen, Microsoft has
22 already started trying to lead you off the path.
23 You'll remember in jury selection a week ago when the
24 Microsoft lawyer and I had a chance to ask everybody on
25 the potential jury panel a few questions, do you

1 remember Microsoft saying to you, well, would everybody
2 agree that during this trial, you won't just assume that
3 the patent is valid? Everybody agree you're just not
4 going to assume that?

5 Ladies and Gentlemen, here's what Judge
6 Davis told you about just this morning. Judge Davis
7 told you, the granting of a patent by the Patent &
8 Trademark Office carries with it the presumption that
9 the patent is valid. The presumption of patent validity
10 imposes the burden on Microsoft to prove invalidity by
11 the clear and convincing evidence standard.

12 Judge Davis told you about that
13 presumption not once, not twice, but three times this
14 morning.

15 And at the very end of the trial, we
16 anticipate that we'll put Professor Jones back on the
17 stand very briefly to explain to you how Microsoft is
18 wrong in its attempt to distract you from the path of
19 fair compensation by claiming that the patents are no
20 good.

21 But if you don't believe that they don't
22 infringe and you don't believe that their infringement
23 was willful and if you don't buy that the patent was
24 invalid, how about this?

25 Microsoft will say the patents really

1 aren't valuable. Nobody wants them.

2 Now, Ladies and Gentlemen, you will
3 hear -- you'll hear it directly from Mr. Munger that he
4 had a difficult time trying to make something out of his
5 invention.

6 Unfortunately, he started off trying to
7 raise money for it, and in the recession of 2000/2001,
8 the last bad recession we had before this one, when
9 technology companies were particularly hard hit, a few
10 years later, he discovers that the largest software
11 company in the world is already using his invention.
12 And from that point forward, you'll hear him explain it
13 was basically hopeless; that this small group of
14 inventors, this small team would be able to compete
15 against a company like Microsoft, that Microsoft wasn't
16 made to respect their patent rights.

17 But that, Ladies and Gentlemen, I'll
18 suggest to you will be the most compelling evidence of
19 how valuable the invention is, because you will hear
20 that the largest software company in the world,
21 Microsoft, uses the invention and has made an enormous
22 amount of money doing so.

23 Now, Ladies of the Jury, I think you've
24 heard about enough from me this morning, and I'm sure
25 you're anxious now to hear this story told by the people

1 who actually lived through it. Mr. Munger will be our
2 very first witness in the trial?

3 And we look forward to introducing him to
4 you shortly.

5 THE COURT: Thank you, Mr. Cawley.

6 All right. Counsel for Microsoft.

7 MR. POWERS: Thank you, Your Honor.

8 THE COURT: Mr. Powers.

9 MR. POWERS: Well, good morning. I
10 appreciate this opportunity from Judge Davis to tell
11 you Microsoft's side of the story.

12 And the interesting thing about it is, we
13 can agree with almost everything that VirnetX's lawyer
14 tells you up until about the last five minutes, the
15 signs-in-the-woods part of the opening statement.

16 Because there really isn't a disagreement
17 in this case about whether security is a good thing,
18 whether patents are a good thing, whether people should
19 pay fair value for their patents. That's -- there's no
20 disagreement about that issue at all.

21 But what I do want to talk to you about
22 is the areas that he called distractions. Remember that
23 the end of the signs? That's the issue that I want to
24 talk about.

25 Because Microsoft believes very, very

1 strongly -- and I'll say it straight out -- that
2 Microsoft does not infringe these patents; that these
3 patents are not valid; and that VirnetX is entitled to
4 no compensation from Microsoft; that is the issue in
5 this case.

6 And we will present the evidence on those
7 issues in this case. But I want to start with
8 explaining, from our point of view, who the key
9 entities, the key companies are in this case.

10 We already heard about all of them -- a
11 little bit about them from Mr. Cawley. He referred to
12 this company, SAIC. Now, SAIC is a very large company.
13 Over 40,000 employees, about \$8 billion in sales.
14 They're a very, very big company.

15 And they primarily sell, as Mr. Cawley
16 said, to the U.S. Government. So they're very relevant
17 to this case, not only because of that, because the
18 technology at issue, which was called NetEraser and then
19 later VernetX by Mr. Munger, that technology was
20 developed at SAIC. So you're going to be hearing a lot
21 about it for that reason.

22 Mr. Munger and Mr. Short were both
23 employees at SAIC at that time, and SAIC filed patent
24 applications that relate to the patents that we're
25 talking about here in this case.

1 But you'll also hear that SAIC attempted
2 very hard to try to get many, many companies interested
3 in that technology. The very same technology you just
4 heard about, Mr. Munger and Mr. Short developed. They
5 worked very hard to try to get people interested in it,
6 and that didn't work.

7 And I want to pause there for a minute,
8 because that shouldn't be a surprise. There's no shame
9 in developing technology that people don't want to buy,
10 because it doesn't really solve a problem, it doesn't
11 work very well or whatever. It happens all the time.
12 Coke developed new Coke. That didn't work very well.
13 Ford developed the Edsel. That didn't work very well.
14 Microsoft developed a lot of those products that just
15 didn't sell very well at all. It happens routinely in
16 this business when you're trying to develop something
17 new, particularly in the technology space.

18 But what you're supposed to do is step
19 back, pick yourself up, and try again. Make something
20 people do want.

21 And Microsoft has been successful. No
22 doubt about it. It's Microsoft's position that it's
23 successful because of its own engineers, it's own hard
24 work.

25 And that success is nothing to be ashamed

1 of. That's a good thing. That's part of what makes
2 this country great, is people making things that keep
3 people employed, that people want to help. That's what
4 it's supposed to be, how it's supposed to work.

5 So there's no shame in the fact that the
6 technology that Mr. Munger and Mr. Short developed
7 wasn't successful commercially. No shame in that. But
8 it is a fact, and I'll show you some evidence that
9 relates to that, because it's important in this case.

10 Finally, SAIC, the very company that
11 employed Mr. Munger and Mr. Short, the very company that
12 filed these patent applications, it decided this
13 technology was not worth further developing, and that
14 decision is supported in this case as well.

15 Here's a list of the companies that SAIC
16 tried to sell to. You see some of the biggest names in
17 the industry: Morgan Stanley, Amazon, eBay, Yahoo,
18 people who were building the internet space, and they
19 took the technology to them, and Mr. Munger was often
20 the person going to give a demonstration and explaining
21 the technology.

22 And these companies, for one reason or
23 another, said: No, no thanks. We're not interested.
24 And that was their decision. And in fact, no company,
25 no company bought the technology that Mr. Munger and Mr.

1 Short developed at that point.

2 Well, they didn't stop there. To their
3 credit, they were persistent, and because SAIC primarily
4 sells to the government, they thought, well, maybe
5 government agencies.

6 You recall the discussion in Mr. Cawley's
7 opening statement that the whole idea of this was to be
8 used for spies and the CIA, so let's try to sell it to
9 the CIA, Homeland Security, the FBI, and many others.
10 And here they had two advantages. One advantage was
11 that SAIC had very good relationships with those
12 agencies. Most of SAIC's business is to sell it to
13 them.

14 But, second, the government already had a
15 free license to these patents because of the N-Q-Tel
16 funding that Mr. Cawley told you about.

17 So you'd think that some of these
18 agencies, if it really solved the problem of security
19 and they could have the license for free, they would
20 have said: Yes, let's use it. Well, they said no, and
21 they said: No. Thank you.

22 Now, that -- again, there's no shame in
23 that. A lot of people, including Microsoft, make the
24 products that people just say no thank you to, but
25 that's a fact.

1 So when you hear VirnetX say that they
2 solved the problem of security, the question would be
3 why did none of these companies, all of which were
4 interested in security, why did they say no thanks?

5 Well, let's talk about N-Q-Tel for a
6 minute, because Mr. Cawley raised it, and that is the
7 place where the initial funding for this work came. You
8 heard that from Mr. Cawley in his opening statement.
9 And you heard about the relationship between N-Q-Tel and
10 the CIA.

11 Well, what you didn't hear was that
12 N-Q-Tel decided to stop the funding, because they gave
13 some initial money before the developmental work
14 started, so before they saw any technology, and then
15 VirnetX, SAIC, delivered that technology to the CIA and
16 said: Here, try it out, and we'd like some more money,
17 please, to finish the development.

18 N-Q-Tel said no. And in language that's
19 fairly clear but harsh, but not my language, N-Q-Tel
20 said: This NetEraser project -- that's the name that --
21 one of the names Mr. Munger had given it -- should be
22 placed in the living dead category -- he put it, not my
23 words -- with little or no attention paid to it.

24 So the very same company that started the
25 funding that was the source of it said, after they saw

1 the technology: No, we're not interested.

2 Well, to their credit, SAIC didn't give
3 up, but then they decided to stop funding as well. And
4 this is a memo from Mr. Munger's boss, Mr. Jobien. This
5 is in June of 2001. And he tells them: Well, the
6 company has pretty much thrown in the towel on
7 NetEraser, now VirnetX.

8 So in 2001, June, they said: Well, we're
9 just not going to fund it anymore.

10 And also in June, this is, again, an
11 internal SAIC document: We're going to pull the plug on
12 VirnetX, which is another name they were using
13 internally for that technology that Mr. Munger and
14 Mr. Short developed.

15 So you have technology that they worked
16 hard to develop. They had a good idea, trying to make
17 things newer, all good so far. They developed it, but
18 it didn't work as well as they wanted it to. It didn't
19 solve the problem that people wanted it to.

20 And, therefore, the original funders
21 said: We're not interested anymore. Their own company
22 said: We're throwing in the towel.

23 But interestingly, there's -- part of the
24 reason was why. So in this memo from Mr. Hendrix, who's
25 a SAIC executive, he says why they're pulling the plug.

1 He says: The straw that broke the camel's back was the
2 loss of the ANX beta site as they decided to go with an
3 Aventail solution.

4 Now, ANX was a company that SAIC had a
5 relationship with, and ANX chose a different technology
6 over Mr. Munger's and Mr. Short's. They chose something
7 called Aventail.

8 And you're going to hear more about that,
9 because that's one of the pieces of prior art that's at
10 issue in this case. It's another technology by another
11 company that solved that VPN security problem.

12 And SAIC, Mr. Munger and Mr. Short's own
13 employers, chose it instead of the Munger/Short
14 technology. And they went beyond that. SAIC actually
15 invested in Aventail. Where SAIC stopped funding the
16 VernetX's technology, they decided to fund Aventail
17 instead.

18 Remember that when we get to the
19 discussion about prior art and validity, because
20 Aventail is very, very important to that.

21 Now, you heard about SafeNet in the
22 opening statement from VirnetX's lawyer. And you heard
23 about a license that SafeNet had with SAIC. And that's
24 all true.

25 But what you didn't hear is that once

1 SAI -- once SafeNet got the technology, the Munger-Short
2 technology, and looked at it and evaluated it, they
3 said: Does it really solve the problem? Does it really
4 work? No, it doesn't actually accomplish any real
5 simplicity. And as they put it: It just moved the
6 complexity around.

7 So all that discussion you heard about
8 trying to make everything simpler, the company that
9 actually had the chance to sell that technology, wanted
10 to sell that technology, because it really worked, after
11 evaluating the technology, said it doesn't really work.
12 And what did they do? They paid VirnetX, under that
13 license agreement that you heard about in opening
14 statement? No. They terminated it before they had to
15 pay them a dime under that 20 percent. No payments
16 under that 20 percent, because the technology didn't
17 work.

18 Now, you heard about the letters that
19 SAIC sent to Microsoft, but there's one part of that
20 story you didn't hear. It is true that after deciding
21 to stop funding their own technology and after being
22 rejected in other attempts to find the funding and
23 customers for it, at that point, they did send a letter
24 to Microsoft saying: We think you infringe.

25 And here's that letter in May of 2006.

1 And it says: We think this patent covers any
2 internet-based communications implementing a particular
3 RFC.

4 RFC is a type of standard in this
5 business, and you'll hear more about that.

6 Well, you'll find out that that statement
7 proved not to be true, the one they said in the first
8 letter accusing us of infringement. We wrote back very,
9 very promptly, just two or three days later, saying:
10 Well, we disagree, but we'd like to meet.

11 We wrote again in September of the same
12 year. We still disagree then and now, but we'd like to
13 meet. But even more than that, we want some information
14 that backs up your claim. Give us something that backs
15 up your position, the claim you made that we infringe.

16 Now, we think that a company that's going
17 to come here and ask for \$42 million would at least send
18 us something saying why they thought we infringed or at
19 least meet with us.

20 They gave us no information. They had no
21 meeting. What they did was sue us, VirnetX. VernitX,
22 Inc., was a company started in 2004 by this man named
23 Kendall Larsen. He owns about 20 percent of the company
24 or a little bit more, and he received the patents from
25 SAIC to go sue Microsoft.

1 So after having the -- SAIC trying to
2 make the company work, not being able to succeed, this
3 is where they went next. VernetX has never sold a
4 product, never.

5 Now Microsoft. Microsoft, I think we all
6 know a lot about. They've been around for a long time
7 now. They employ a lot of people and they have a great,
8 great history of innovation in this space. They have
9 over 26,000 engineers working very, very hard to create
10 the products that we all use every day.

11 They're proud of that; we're proud of
12 that. Now, the problem with that -- their success is
13 often -- one of the people we're going to meet that you
14 already met in jury selection is Gurdeep Pall. Gurdeep
15 joined Microsoft in 1990.

16 Thank you, Gurdeep.

17 And he is one of the true pioneers in VPN
18 technology. And VPN technology works, and people
19 actually use it. He's a Vice President at Microsoft,
20 and he coined something called Pointe2Pointe
21 Tunneling Protocol.

22 And that was the first commercial VPN.
23 Called PPTP. Unfortunately, you get a lot of acronyms
24 in this case. I can't do anything about it. That's how
25 these people speak.

1 But PPTP, which is hard to say five times
2 fast, that was the first commercial successful VPN,
3 virtual private network, and Mr. Pall coinvented that at
4 Microsoft.

5 He also invented a technology called
6 AutoDial, which is pretty much exactly what it sounds
7 like, something which automatically makes a connection,
8 very similar to what you're talking about, and that
9 happened before Mr. Munger did his work. All of that
10 happened before Mr. Munger did his work.

11 Mr. Pall has been recognized by many
12 people, including Information Week, as being one of the
13 premier technologists of our time working on this
14 problem. He was called one of 15 innovators who will
15 make a difference in 2008. Yet he's the one who stands
16 here accused of being an infringer. He's a true
17 innovator.

18 Let me back up some of what I just said.
19 You heard from Mr. Cawley that in 2000, SAIC filed those
20 patent applications. Now, when did Mr. Pall, Gurdeep
21 Pall, do his PPTP VPN? Way back in 1996. Four years
22 earlier. That's when he invented it and released it.
23 And AutoDial came out later that year, four years
24 earlier, a long time ago. He was working on that well
25 before Mr. Munger even started, much less before they

1 had the invention.

2 Now, what was PPT -- PPTP -- can't even
3 say it -- what is it and how did it work and why is it
4 important? Well, it did really change how we work. It
5 allowed easy access to a company network.

6 And you'll hear from Mr. Pall that one of
7 the things he was thinking about when he was inventing
8 this was how filled the Microsoft parking lot was at
9 midnight. Everybody had to get their work done. They
10 work very, very hard there, and they were working
11 sitting in their cubicles working at midnight.

12 And he says: Wouldn't it be nice if we
13 could work at home? That way we could go home, see our
14 families, have dinner, and then work at home without
15 having to stay here all night long. And that's one of
16 the things he was trying to solve.

17 And sure enough, after he invented PPTP,
18 that parking lot, never empty, was a lot, lot less
19 filled at midnight. Because then people could work at
20 home and do it easily, and they could do it securely.

21 Now, it's not just me saying that; the
22 world recognized this advance. PC magazine, in December
23 of 1996, gave Mr. Gurdeep Pall's Pointe2Pointe Tunneling
24 Protocol the Networking Software Technical Excellence
25 Award.

1 And what did they say about it? They
2 said: It's a new protocol that enables secure remote
3 access across the public internet, exactly what we're
4 talking about here, exactly what VirnetX's lawyers say
5 they saw in 2000, 1999. PC week is saying Mr. Pall did
6 it in 1996.

7 But more than that, excellent security
8 PPTP provides, and it's a virtual private network while
9 locking out unauthorized users. All of that in 1996,
10 four years before.

11 So what is this case about from
12 Microsoft's perspective? Let me talk about first what
13 we don't think it's about. It's not about whether
14 patents are good. Microsoft agrees, patents are a good
15 thing.

16 It's not about whether people who have
17 patents should be paid fair value when someone uses
18 those. We agree. And in fact, you'll hear in the
19 evidence we do pay fair value when we use someone's
20 technology. You'll hear about a lot of licenses that we
21 took and said we're paying fair value.

22 It's not about whether -- it's not about
23 whether security is a good thing. Security is a good
24 thing and will be a problem. It has been forever, and
25 it will be forever.

1 Every time you get an advance, there's
2 still someone trying to make everything more secure.
3 But the idea that the problem of security was solved in
4 1999 by Mr. Munger and Mr. Short's work, however hard
5 they worked, it just isn't true. We're always working
6 on better security. Always. But that's not the issue
7 here.

8 It's also not about whether Mr. Munger
9 should be saluted and thanked by everyone here for his
10 war story. Everyone agrees with that. That's not the
11 issue either.

12 The issues in this case, the ones that
13 will be on the verdict form that Judge Davis mentioned
14 to you, are really going to be three, and there are
15 going to be a lot of issues that can be raised in the
16 patent case, but I'm only going to talk about three, and
17 these are the three core issues.

18 First, does Microsoft software, the ones
19 they're saying infringe, does that software use the
20 VirnetX's patent?

21 Second, was VirnetX first? You heard
22 Judge Davis' instructions about anticipation. That's
23 what this question is about. If somebody did what
24 VernetX claimed but did it earlier, the patent's not
25 valid.

1 And last, was VernetX's claimed invention
2 obvious? But not just obvious to anyone; obvious to
3 those skilled in this technology.

4 And that's an important distinction that
5 I want to pause on for just a minute, because something
6 that's obvious to somebody might not be obvious to
7 others if they don't have the same training or
8 experience.

9 We're coming up on tax season, and you
10 could say whether something is deductible is not always
11 obvious to me, but it would be obvious to an accountant
12 who works in that space every day. You could say that a
13 certain symptom that caused that symptom is not always
14 obvious to me but would be obvious to a doctor or nurse
15 who works in that field.

16 You could ask whether the reason for a
17 teenager's behavior is obvious? Well, if you have five
18 kids as I do, three of them teenagers, might be a little
19 more obvious than to somebody who's never had a kid.
20 And the whole point of that is, obviousness has to be
21 viewed through the eyes of the person that's relevant.
22 And here the person that's relevant is someone who has a
23 lot of training in this exact space, a lot of education,
24 and a lot of experience.

25 So much more is obvious to them than

1 would be obvious to almost anyone else in this
2 courtroom.

3 Let's talk about the first issue first.
4 Microsoft software does not use the VirnetX patent.
5 Our first two witnesses are going to be Gurdeep Pall,
6 who you've met, and Tyler Barton, another Microsoft
7 employee who worked on these technologies.

8 Tyler, would you stand up, please?

9 And they will explain to you what they
10 did, how it works. They'll tell you about that
11 technology, and that will be from the people who
12 actually invented it and made it work.

13 You'll also hear from Professor David
14 Johnson, who's an expert in this space.

15 Mr. Johnson, could you stand up?

16 And he'll explain to you his analysis,
17 after many, many hours, why Microsoft does not infringe.
18 But I don't want to give you just conclusions; I want to
19 show you the evidence and why Microsoft's products don't
20 infringe. They don't use VernitX's patents. And
21 there's two core reasons.

22 You heard from Judge Davis' instructions,
23 and you'll hear later, that in order to show
24 infringement, VirnetX has the burden to show every
25 single aspect of those claims is contained in our

1 software. If it's missing only one, there's no
2 infringement. And we're showing you two as to the '135
3 patent.

4 First question is whether they're VPNs.
5 Now, Judge Davis has given you instructions on what a
6 VPN means on that first sheet in the juror notebook,
7 and this is a copy of it right here from your juror
8 notebook. And the key point is, there has to be private
9 communication.

10 So you might say, well, how do I know
11 whether it's private? Well, you know whether it's
12 private in two ways.

13 And the way it's important here is
14 whether someone is eavesdropping on a communication,
15 we'll know who's talking to whom. And for that, I have
16 to spend just a little bit of time explaining some of
17 what this technology is going to be about.

18 One of the products in question is
19 Microsoft's Office Communicator, also called OC or OCS.
20 In that context, this requirement that an eavesdropper
21 can't tell who's talking to whom doesn't matter, and
22 I'll show you why.

23 Now, in any communication on the
24 internet, you see these numbers here on the left,
25 204.11.52.127 and the different numbers over on the

1 right? Those are called IP addresses.

2 And that's going to be one of the most
3 important concepts in this case, an IP address. Because
4 for a computer, an IP address is like a name.

5 So if these were two people talking, it
6 might be Matt Powers talking to Gurdeep Pall. But in
7 the case of computers, you use numbers because that's
8 what computers work on.

9 And so the issue back when the computer
10 on the left talks through that internet to the computer
11 on the right, can an eavesdropper see who's talking to
12 whom? And the answer here, as you see, is that
13 eavesdropper can see exactly those numbers, and they're
14 the same numbers.

15 What you'll hear from VirnetX is that
16 their idea was, you prevent that eavesdropper from
17 seeing the IP addresses.

18 So the big issue here is, can
19 eavesdroppers see those numbers, the numbers
20 corresponding to the real numbers of those computers?

21 If the answer is yes, there's no
22 infringement, because it's not an -- it's not secret.
23 It's not private. If the answer's no, then that
24 limitation is met.

25 And you'll hear from VirnetX how they

1 tried all sorts of ways to prevent that eavesdropper
2 from seeing those numbers, including using different
3 numbers so that they could see maybe some numbers but
4 not the right numbers.

5 But in our technology, because it's not
6 being used with spies and CIA, but being used by normal
7 folks sitting in our houses, those numbers are visible.

8 Now, there are many other things done for
9 protection and security, but you can see those numbers,
10 so there's no infringement.

11 Now, you might ask yourself, what does
12 Microsoft say when it's trying to sell this Office
13 Communicator Product? Do we say it's great because of
14 the VPN, and therefore, it's secure?

15 Well, actually, we tell you the opposite.
16 It doesn't require a VPN, and it needs only an internet
17 connection. So it's the opposite.

18 So that VPN requirement of the claims
19 just one of the things that VirnetX has to prove, it's
20 just not there.

21 The second requirement that you'll see in
22 the claims is that there be a website. Well, Microsoft
23 products aren't websites. And, again, Judge Davis has
24 given us a definition. That's in the front page of your
25 book, and it says it's related web pages on the

1 worldwide web.

2 Well, we all know what web pages are. We
3 use them often every day, whether it's Facebook, whether
4 it's Google, whether it's Bing, any one of those, we use
5 those every day, and that's a web page. You know what
6 those are.

7 And the worldwide web, which is that www
8 in the name, well, that's just a collection of all those
9 web pages. They're all linked together, and the reason
10 it's called a web is it sort of looks like a web like
11 you would envision. That's why it was called web.

12 Now, this accused product, this OC/OCS,
13 the Office Communicator, that's not a website. That's
14 software that is running on a server.

15 Now, VernetX here has admitted it's not a
16 website, even though that's a key requirement of the
17 claim. So VernetX has been forced to admit there's no
18 literal infringement.

19 So what they're arguing is that OCS is
20 equivalent to a website, and that will be an issue that
21 you have to decide on this particular requirement.
22 But it's important, from our point of view, that you
23 understand that under their theory, almost everything is
24 a website, even a phone. Even a phone can be a website
25 under their definition or an equivalent to a website.

1 And I think that sort of argument tells you exactly what
2 their position is.

3 So there are two requirements to that
4 '135 patent that they have to prove, two requirements,
5 and both of them are missing. If only one is missing,
6 they cannot prove infringement.

7 So now let's talk about the '135 patent,
8 again looking at the detail. Not the conclusion, but
9 the actual facts.

10 Two requirements here, too. First, that
11 same requirement of VPN. The second is something called
12 a secure computer network address. You'll be hearing a
13 lot about both of those.

14 Now, the VPN, same issue. The question
15 is whether that -- these particular IP addresses can be
16 seen by an eavesdropper.

17 Well, in Windows Meeting Space, which is
18 a particular product -- the application that's at issue
19 on this patent, '180, no dispute that that number and
20 that number are both the -- you can't see them. And
21 remember, if you can see those numbers, there's no
22 infringement.

23 So VPN isn't satisfied for the '180
24 patent for the same reason it wasn't satisfied in the
25 '135. It's not private. You can see the right numbers,

1 the right names of those computers.

2 But there's a second requirement, this
3 secure computer network address. That requires
4 authorization for access. That's Judge Davis'
5 definition. And so the question is, on the products
6 that they're talking about for the '180 patent, does the
7 address require authorization for access?

8 Well -- and it's important to understand
9 what that means, because in the context of a computer,
10 you could have a computer, for example, at a big
11 company, where you're behind what's called a firewall.
12 And you cannot get to that computer unless you have
13 access to get through that firewall. That's what
14 protects that company's computers from outside people
15 coming in. It's built up, it's protected, and it
16 requires --

17 That's not what they're accusing here.
18 What they're accusing here, it's saying that our
19 computers at our homes are secure computer network
20 addresses.

21 Well, I don't know about you, but my
22 computer in my home gets a lot of e-mails that I didn't
23 give anybody access to. Advertisements for things I
24 didn't -- I don't want. A lot of what's called spam
25 e-mail.

1 Now, that -- but that address is what
2 they're calling a secure address. A lot of people get
3 information to me on my home address that I don't give
4 any authority to at all.

5 And so when you compare the difference
6 between a secure address and an insecure address, I
7 think a good example is 211 West Ferguson Street, which
8 is the address of this courthouse that we're all in
9 right now. That's a secure address.

10 It's locked at a lot of the time, and
11 when it's not, there's a guard downstairs with a gun.
12 You have to give your driver's license to get in, and
13 then you have to go through a metal detector. That's a
14 secure address. That's like the firewall that I told
15 you about before.

16 My home computer, the one they're
17 accusing here, where people can send spam without my
18 authority, that's like the Wal-Mart. It's open 24
19 hours.

20 Now, 5050 Troup Highway is that address.
21 Is that a secure address? No. Anybody can walk in.
22 Just like my computer at home, anybody can send me an
23 e-mail without me blocking it. That's the difference,
24 and that's not a secure address.

25 So that's the second key requirement in

1 this case that VirnetX has to prove. And if they can't
2 prove any one of them, they haven't made their case.
3 They can't prove that one either.

4 So that's the first question. That's the
5 first question you're going to be asked on the verdict
6 form that Judge Davis gives you. Not a distraction.
7 It's the actual issue in this case. Do we use their
8 patents? The answer is no.

9 Second, was VirnetX first? Again, this
10 is going to be the issue on the verdict form,
11 anticipation. Well, they weren't. They were not first.
12 And here the Patent Examiner did not have the best prior
13 art.

14 And the three I'm going to focus on are
15 Aventail -- you heard about that before -- Microsoft's
16 PPTP with AutoDial -- you heard about that before;
17 that's the one that Gurdeep Pall invented back in '96 --
18 and one you haven't heard about yet called Dynamic VPN,
19 also known as DVPN, that was created by a company called
20 Trusted Information Systems, TIS.

21 Now, I say the Patent Examiner didn't
22 have this prior art. You might say, well, how do I know
23 that? We know that for exactly the reason that Judge
24 Davis you in the earlier instructions. The patents tell
25 you exactly what prior art or what knowledge the

1 Examiner looked at, so we don't have any question about
2 it. He lists it under references cited.

3 And the interesting thing is, it's the
4 same Examiner for both patents, the '135 and the '180.
5 The Examiner was the same person, Krisna Lim. And
6 Aventail PPTP with AutoDial and DVPN, none of those is
7 listed in those references cited.

8 So you are going to be the first group
9 that can decide whether these patents are valid based on
10 that prior art. The Patent Office didn't have a chance
11 to, and under our system, if you remember from the jury
12 video and from Judge Davis' instructions, you're the
13 only group that can decide that. No one else has.

14 Now, you might say, how could that be?
15 How could that be possible? The Patent Office is --
16 that's their job, is to look at all the prior art.
17 Well, the answer to that lies partly in common sense and
18 partly what you heard in the jury video, the jury video
19 that you saw about a week ago. The common sense part is
20 that Patent Examiners are human beings. None of us is
21 perfect. People can make mistakes. That can happen.
22 But you also heard in Judge Davis' instructions just
23 this morning that the Patent Office may or may not have
24 the best prior art. And that's the case here. Because
25 we know the Patent Office didn't consider those three

1 references.

2 But you also saw in the jury video these
3 pictures and saw that -- and heard this discussion, and
4 you saw they had a lot of work to do.

5 Now, we're not saying they don't try
6 their best, and we're not saying they make a mistake all
7 the time. No. We're just saying, it's possible that in
8 this context, they didn't have the best prior art to
9 make the decision that you have to make. And that's
10 exactly what happened in this case.

11 So the first piece of art I want to talk
12 to you about is Aventail. I actually had to look it up.
13 Their logo is a knight on a horse.

14 Aventail -- and the reason they named it
15 that, and you'll hear about this from one of the
16 witnesses -- it's a type of armor that each of the
17 knights used when they were jousting. So it involves
18 protection, and that's why they chose the name. I
19 thought that was interesting.

20 You'll hear from Chris Hopen by videotape
21 deposition. He's not a Microsoft employee. He's the
22 one that founded Aventail, the company. And you'll hear
23 from him about when -- what he did, when he did it, and
24 how it works.

25 And you might ask yourself, who was

1 first? Was Aventail first, or was Mr. Munger or
2 Dr. Short first? Well, here's their application in
3 2000.

4 Way back here in 1996, Mr. Hopen founded
5 Aventail, four years earlier, and they actually had a
6 product that people were selling and that many, many
7 large companies, including many of the large companies
8 that SAIC tried to sell to, who wouldn't buy it, they
9 were using Aventail, and those sales started in late
10 1997.

11 But there's one other aspect about
12 Aventail that's important in this case. It's not just
13 that they were first and that they were selling actual
14 products that people were using that worked; it's that
15 SAIC in this case actually chose Aventail over its own
16 technology.

17 Remember, the SAIC employees were
18 Mr. Munger and Mr. Short, and they chose Aventail for
19 the ANX beta site -- ANX did -- and SAIC chose to invest
20 in Aventail rather than to further fund the work that
21 Mr. Munger and Mr. Short were doing.

22 And that tells you a lot about whether
23 Aventail was the earlier inventor because SAIC had the
24 chance to pick either, and it chose Aventail.

25 You'll hear from Professor Wicker, an

1 expert witness in this case who's been very, very
2 involved in the areas that matter. And it could be
3 we'll talk about the DARPA, because that called the
4 Defense Advanced Research Projects Agency.

5 It's affiliated with the Department of
6 Defense, and their job is to do research and support
7 research that relates -- that can support the Department
8 of Defense. You're going to be hearing about that quite
9 a bit.

10 Dr. Wicker was involved in that. Also
11 involved in the National Science Foundation Cyber
12 Security Center, which is called TRUST. And he's done a
13 lot of work in this case.

14 Dr. Wicker, would you stand up? Thanks.

15 And you'll hear from him as to why, in
16 his view, based on these specific references, it's
17 invalid.

18 And I'm not going to -- I don't have the
19 time to show you all that entails. He's certainly much
20 better able to explain it than I am. But if you take
21 the claim, and you divide it up into its various pieces,
22 he will show you how each aspect of that claim is
23 specifically found and executed in Aventail. He will
24 show how every aspect of the claim works and how
25 Aventail did it but did it before SAIC.

1 The second piece of prior art I want to
2 talk about is Gurdeep's PPTP with AutoDial.

3 The first question, of course, is going
4 to be, is it first? Because it's not prior art if it's
5 not earlier. We have the same 2000 date where they
6 filed their applications.

7 When did he do this work? We already
8 know the answer to that. He did it back in 1996. But
9 he didn't stop in '96. He kept improving it, and he got
10 better and better, all before the patent application by
11 SAIC.

12 NT5 was released in 1997. NT4, you're
13 going to hear a lot about that. That's just the
14 internal Microsoft name for that product. That was in
15 '96. It's a real product. People were really buying
16 it, using it, working. NT5, two years later, an
17 improvement.

18 The Beta 3 released in 1999, yet all
19 before, all before the work that we're talking about by
20 Mr. Munger and Mr. Short.

21 So then the question is: We know it's
22 earlier. What did it do?

23 Again, Dr. Wicker -- Professor Wicker
24 will explain to you in detail how that prior art
25 invalidates both patents-in-suit, because it did earlier

1 what they claim to have done later, which is really just
2 the issue.

3 And, again, he'll do that comparing the
4 claims, showing you, based on the figures of PPTP, how
5 every aspect of that claim is found exactly in the
6 reference PPTP and how PPTP works. But it was four
7 years earlier.

8 So the four pieces of prior art that
9 we're going to be talking about is this Trust &
10 Information Systems Company's product called DVPN or
11 Dynamic VPN. And you'll hear from three witnesses on
12 this. None of them are a Microsoft witness, because
13 it's not a Microsoft type of product.

14 The first is a man named Sami Sajdjari.
15 Now, he works for DARPA, that company I just mentioned a
16 little bit ago. And DARPA plays in this quite a bit.
17 It's interesting. Mr. Sajdjari actually led a
18 conference in February of 1998 that Mr. Munger attended
19 that got him to really thinking about how to build a
20 product here.

21 That was in February of 1998. Mr.
22 Sajdjari was the one leading that meeting, and then Mr.
23 Munger submitted a proposal to DARPA asking for funding.

24 Now, you'll also hear from Dan Sterne and
25 Darrell Kindred, both who work for that Trust &

1 Information Systems Company, about what the product is
2 and what it did.

3 And you'll also learn that it was well
4 before. Same patents in 2000. Trust & Information
5 Systems development started in '97 and actually showed
6 that product at a DARPA conference in March of 1998,
7 long before.

8 So it's clearly prior art.

9 And you'll also hear from both Mr.
10 Sajdjari and Mr. Sterne that DARPA funded the TISC DVPN
11 work; yet they rejected SAIC's request that DARPA fund
12 Mr. Munger's work. They chose TISC's product and
13 technology over Mr. Munger's and Mr. Short's. And
14 you'll hear from Professor Wicker on that subject as
15 well.

16 Now, the third and last issue is
17 obviousness. And remember, obviousness is obvious to
18 this person who's skilled in the area of the technology,
19 not to really any of us. And you'll hear from experts
20 on that issue.

21 So the first reason the patents are not
22 valid, the biggest one first. That's a basic
23 requirement of U.S. patent law, as Judge Davis has
24 instructed you.

25 But we're also going to show you

1 obviousness, and obviousness goes to what people in this
2 field were doing at that time.

3 And the interesting thing about this
4 field is that it's not a couple of people in garages
5 sort of working by themselves. You can imagine you
6 wouldn't want that, if you're talking about how the
7 system, the entire internet is going to work.

8 So there's an organization called the IP
9 IETF, Internet Engineering Task Force, and that is a
10 very large organization made up of some of the best
11 minds, from professors, companies, government,
12 et cetera, who all come together and think about how the
13 internet should work, which makes sense that you would
14 want to all work together, so they need to follow all
15 the same rules.

16 And you'll find out that the concepts in
17 these SAIC patents were well, well known in already
18 established standards at the time. Already established
19 standards.

20 And those groups, the IETF, got together
21 and said -- they're trying for more security. Let's try
22 these various efforts, and you'll hear about those
23 different standards.

24 Damages. Short answer from Microsoft's
25 perspective is there are none. We don't infringe, and

1 the patents are invalid.

2 When we talk about what this case is
3 about, the first issue, does Microsoft's software use
4 the VirnetX patent, the ones that they're saying we do
5 and they're saying they infringe? Well, no.

6 That eavesdropper can see the address,
7 the right address of those computers. And therefore,
8 it's not anonymous and not private. It's not a VPN.
9 It's certainly not a website and not a secure address.
10 Not like this courthouse. It's more like the Wal-Mart,
11 our computers at home.

12 Was VernetX first? They were four years
13 behind other people and four years behind other people
14 whose technology was working, being sold and bought and
15 used out there in the world at a time when SAIC's
16 technology people were saying: No thank you.

17 So does Microsoft software use the
18 VirnetX patents? The answer to that is no.

19 Was VirnetX first? No. They were four
20 years behind at least these three companies.

21 And was VirnetX's claimed invention
22 obvious? The answer to that is yes.

23 So based on the evidence, based on the
24 facts -- not distraction, but based on the actual issues
25 you have to decide, we will ask you to render a verdict

1 for Microsoft.

2 I thank you very, very much for your
3 attention.

4 THE COURT: Okay. Thank you, Mr. Powers.

5 All right. Ladies of the Jury, you've
6 now heard the opening statements in the case, as well as
7 the Court's preliminary instructions. We're going to
8 recess for lunch at this time, and we'll come back after
9 lunch and begin hearing the evidence in the case.

10 So I'm going to recess you until 1:30
11 today, give you a little extra time. Normally, we'll
12 take about an hour, hour and 10 minutes. I'm going to
13 give you about an hour and 25 minutes today, give you a
14 chance to get familiar with downtown, find your
15 restaurants you want to eat at, and get you some lunch.

16 And be back here ready to go at 1:30.

17 Please remember my instructions. Don't
18 discuss the case among yourselves or with anyone else.
19 Just keep your own countenance about the case until all
20 the evidence comes in. So enjoy your lunch, and the
21 jury is excused at this time.

22 COURT SECURITY OFFICER: All rise for the
23 jury.

24 (Jury out.)

25 THE COURT: Please be seated.

1 All right. If you would, if you're in
2 the audience, if you could just remain in the courtroom
3 until we finish the hearing.

4 Ma'am, if you would just -- ma'am, if you
5 would just remain in the courtroom until we finish the
6 hearing. What I want to do is give the jury a chance to
7 get out before everybody starts exiting, give them a
8 head start on lunch ahead of all of you.

9 Let me just go over with the parties,
10 when we come back after lunch, one of the first things I
11 would like to do is have the exhibits introduced, and
12 we'll go through that exercise first.

13 And then I'll have -- I'd like for you to
14 have all of your witnesses in the room so that they can
15 all be sworn in at one time. We won't have to do that
16 piecemeal.

17 If they're not here today, then we'll
18 swear them in as we deal with them, but everybody that's
19 available today and here, please have them in the
20 courtroom, and we'll swear them in.

21 Is either side going to invoke the Rule?

22 MR. POWERS: Yes, Your Honor.

23 THE COURT: Okay. Have y'all discussed
24 and worked out an agreement as far as who is excused
25 from the Rule?

1 MR. CAWLEY: Actually, we haven't. I
2 assume expert witnesses.

3 MR. POWERS: Exactly.

4 MR. CAWLEY: Okay.

5 THE COURT: Expert witness, and we know
6 who our company representatives are.

7 Anybody else in dispute?

8 MR. POWERS: There's no dispute, Your
9 Honor.

10 THE COURT: Okay. All right. Well, just
11 be sure y'all explain to your witness who's covered and
12 who's not, and I won't try to go through that in front
13 of the jury.

14 All right. Anything else before we break
15 for lunch?

16 MR. CAWLEY: None from the Plaintiff.

17 MR. POWERS: None from Microsoft.

18 THE COURT: Okay. Very well. Well, let
19 me ask you again about this motion to strike. When does
20 that need to be taken up by?

21 MR. CALDWELL: Your Honor, I guess it
22 depends on when Microsoft wants to -- if they're going
23 to put on evidence in front of the jury. I mean, it's a
24 legal defense, so I don't know that they're going to put
25 on evidence in front of the jury, but I'm -- I'm not

1 sure I can answer.

2 MR. POWERS: As we said in the papers,
3 Your Honor, we believe it's a legal defense. We're not
4 putting on evidence in front of the jury about it. It's
5 an issue for the Court.

6 THE COURT: Well, I'll continue to
7 consider it then.

8 All right. Be in recess.

9 COURT SECURITY OFFICER: All rise.

10 (Lunch recess.)

11 * * * * *

12

13

14

15

16

17

18

19

20

21

22

23

24

25

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

CERTIFICATION

I HEREBY CERTIFY that the foregoing is a true and correct transcript from the stenographic notes of the proceedings in the above-entitled matter to the best of my ability.

/s/ _____
SUSAN SIMMONS, CSR
Official Court Reporter
State of Texas No.: 267
Expiration Date: 12/31/10

Date

/s/ _____
JUDITH WERLINGER, CSR
Deputy Official Court Reporter
State of Texas No.: 731
Expiration Date: 12/31/10

Date

EXHIBIT F2

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

1			
2			
3	VIRNETX	*	Civil Docket No.
4		*	6:07-CV-80
5	VS.	*	Tyler, Texas
6		*	March 8, 2010
7	MICROSOFT CORPORATION	*	1:30 P.M.

TRANSCRIPT OF JURY TRIAL
BEFORE THE HONORABLE JUDGE LEONARD DAVIS
UNITED STATES DISTRICT JUDGE

APPEARANCES:

12	FOR THE PLAINTIFFS:	MR. DOUGLAS CAWLEY
13		MR. BRADLEY CALDWELL
14		MR. JASON D. CASSADY
15		MR. LUKE MCLEROY
16		McKool-Smith
17		300 Crescent Court
18		Suite 1500
19		Dallas, TX 75201
20		MR. ROBERT M. PARKER
21		Parker, Bunt & Ainsworth
22		100 East Ferguson
23		Suite 1114
24		Tyler, TX 75702

APPEARANCES CONTINUED ON NEXT PAGE:

22	COURT REPORTERS:	MS. SUSAN SIMMONS, CSR
23		Ms. Judith Werlinger, CSR
24		Official Court Reporters
25		100 East Houston, Suite 125
		Marshall, TX 75670
		903/935-3868

(Proceedings recorded by mechanical stenography,
transcript produced on CAT system.)

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

APPEARANCES CONTINUED:

FOR THE DEFENDANT: MR. MATTHEW POWERS
MR. JARED BOBROW
MR. PAUL EHRLICH
MR. THOMAS KING
MR. ROBERT GERRITY
Weil Gotshal & Manges
201 Redwood Shores Parkway
5th Floor
Redwood City, CA 94065

MS. ELIZABETH WEISWASSER
MR. TIM DeMASI
Weil Gotshal & Manges
767 Fifth Avenue
New York, NY 10153

MR. DANIEL BOOTH
Weil Gotshal & Manges
700 Louisiana
Suite 1600
Houston, TX 77002

MR. RICHARD SAYLES
MR. MARK STRACHAN
Sayles Werbner
1201 Elm Street
4400 Renaissance Tower
Dallas, TX 75270

MR. ERIC FINDLAY
Findlay Craft
6760 Old Jacksonville Highway
Suite 101
Tyler, TX 75703

* * * * *

P R O C E E D I N G S

COURT SECURITY OFFICER: All rise.

(Jury in.)

THE COURT: Please be seated.

All right. Everybody ready to go?

1 Okay. All right. Let's see. First,
2 we're going to have all the witnesses that are going to
3 testify. So if you're a witness who's going to testify
4 in this case, if you would please stand wherever you
5 are.

6 All right. And if you would start here
7 at the front and just state your name on around the
8 room, so the court reporter can take it down.

9 A WITNESS: My name is Edmund Colby
10 Munger.

11 A WITNESS: My name's Gurdeep Singh-Pall.

12 THE COURT: Would you spell that.

13 A WITNESS: Yes. G-U-R-D-E-E-P,
14 S-I-N-G-H, and last name is P-A-L-L.

15 THE COURT: Thank you very much.

16 Okay. Next?

17 A WITNESS: My name is Tyler Barton.

18 THE COURT: And how do you spell that
19 last name.

20 A WITNESS: B-A-R-T-O-N.

21 THE COURT: Okay.

22 A WITNESS: My name is David Johnson.

23 A WITNESS: My name is Stephen Wicker.

24 A WITNESS: Mark Thomas Jones.

25 A WITNESS: Brett Reed.

1 A WITNESS: Robert Dunman Short.

2 THE COURT: Short?

3 A WITNESS: Short, yes.

4 THE COURT: If you would raise your right
5 hand to be sworn.

6 (Witnesses sworn.)

7 THE COURT: Now each of you have been
8 sworn as witnesses in this case. The Rule has been
9 invoked, and that means if you're a witness and you're
10 not a party representative and you're not an expert,
11 then you cannot be present during the proceedings and
12 would need to leave the courtroom.

13 Also, you cannot discuss the case with
14 anyone else during the course of the case, other than
15 one of the attorneys associated with the case.

16 So if you're one of the parties that is
17 not -- or if you are a witness who is not an expert or
18 who is not a representative of a party, you would need
19 to leave the courtroom at this time; otherwise, you may
20 be seated.

21 All right. At this time, does Plaintiff
22 have some exhibits that it wishes to offer?

23 MR. McLEROY: Yes, Your Honor, we do.
24 Should I read them into the record, Your Honor?

25 THE COURT: How long is it?

1 MR. McLEROY: It's a long list.

2 THE COURT: Long list? Let me see a copy
3 of them, if you would.

4 All right. This is entitled, List of
5 Plaintiff's Trial Exhibits to be Admitted.

6 Has Defendant Microsoft had an
7 opportunity to review this list, which is 15 pages in
8 length, and begins with No. 1 and ends at No. 983?

9 MR. POWERS: We've been exchanging lists
10 of what's objected to, and I believe this list to be
11 accurate, so there is no objection.

12 THE COURT: I am going to mark this as
13 Plaintiff's Exhibit List No. 1 just for purposes of the
14 court record.

15 Do you have any objections to any of the
16 exhibits listed in this?

17 MR. POWERS: We do not, Your Honor.

18 THE COURT: So the exhibits listed in
19 Plaintiff's Exhibit List No. 1 will be admitted,
20 Ms. Ferguson.

21 Does the Defendant have any exhibits it
22 wishes to offer?

23 MR. POWERS: Similarly, Your Honor.

24 THE COURT: All right.

25 All right. I have been handed what's

1 marked, List of Defendant Microsoft's Trial Exhibits to
2 be Admitted. And this is some 21 pages in length, and
3 begins with Exhibit No. 3001 and goes through 3576.
4 And I will tell the Members of the Jury that these
5 numbers aren't all consecutive, so there's not that many
6 exhibits; it's just in -- just the numbering system for
7 both parties.

8 All right. I will mark this as
9 Defendant's Exhibit List No. 1.

10 Does Defendant offer all of these
11 exhibits?

12 MR. POWERS: We do, Your Honor, and,
13 similarly, I will represent that these are the exhibits
14 that Plaintiff has said they have no objection to.

15 THE COURT: And does Plaintiff have any
16 objection?

17 MR. McLEROY: Your Honor, excepting the
18 representation, we have not had a chance to look at this
19 list before, so we have not had a chance to double-check
20 to make sure --

21 THE COURT: All right. Exchanging lists,
22 and you have no reason to believe this is not the list?

23 MR. McLEROY: No, Your Honor. We have
24 not exchanged this list before.

25 MR. POWERS: We have exchanged similar

1 list, but this is just a combined list of the lists that
2 went back and forth. I will represent that.

3 THE COURT: Do you have any objections to
4 the exhibits listed on Defendant's Exhibit List No. 1.

5 MR. McLEROY: No, Your Honor, we don't.

6 THE COURT: All right. Be admitted.

7 MR. POWERS: Your Honor --

8 THE COURT: And if -- if -- go over it
9 and if as represented, there are any that aren't, bring
10 it to my attention this afternoon, and I will reconsider
11 those.

12 MR. McLEROY: Yes, Your Honor.

13 MR. POWERS: I will note for the record
14 that our agreement that these are in evidence is subject
15 to the stipulation that we earlier submitted to Your
16 Honor that you haven't yet ruled, but it is subject to
17 that issue.

18 THE COURT: I understand. All right.
19 Okay. With that, Plaintiff may call their first
20 witness.

21 MR. CAWLEY: Thank you, Your Honor.
22 Plaintiff VirnetX would like to call to the stand
23 Mr. Gif Munger.

24 THE COURT: All right. Mr. Munger.

25 MR. CAWLEY: Your Honor, may I approach

1 with a document?

2 THE COURT: You certainly may.

3 MR. CAWLEY: May I proceed, Your Honor?

4 THE COURT: Yes, you may.

5 EDMUND "GIF" MUNGER, PLAINTIFF'S WITNESS, PREVIOUSLY

6 SWORN

7 DIRECT EXAMINATION

8 BY MR. CAWLEY:

9 Q. Would you please introduce yourself to the
10 jury.

11 A. Yes, sir. I am Edmund Colby Munger, and I
12 have a nickname Gif.

13 Q. Why are you here, Mr. Munger?

14 A. I'm one of the co-inventors on the two patents
15 that are in question.

16 Q. What did you invent?

17 A. The invention makes it easier to communicate
18 across the internet safely.

19 Q. Did you get patents for your invention?

20 A. Yes, sir.

21 Q. Is your invention important?

22 A. Yes, sir.

23 Q. Why do you say that?

24 A. All right. It's important that it's easy to
25 set up VPN connections so we can protect -- protect

1 communications across the internet, whether they be
2 pictures or files.

3 Q. What kind of people would use your invention?

4 A. Well, anybody could use the invention. Any
5 individual, moms could move her pictures, but also small
6 businesses could use it to communicate their sensitive
7 data, large corporations, and even the government.

8 Q. Could it help even people who don't personally
9 use computers?

10 A. Yes, sir.

11 Q. How is that?

12 A. Well, anytime you go into a store or use a
13 credit card, the information that you provide is --
14 is -- is private, and that data is moved around by
15 networks between banks to set up credit cards. And so
16 businesses use it to order and transmit sensitive
17 information.

18 Q. Now, Mr. Munger, did you invent this by
19 yourself?

20 A. No, sir. It was a team.

21 Q. Tell us who -- who else was on the team.

22 A. There was Dr. Bob Short, Dr. Vic Larson,
23 Dr. Doug Schmidt, and Michael Williamson.

24 Q. And are they all listed as inventors on the
25 patent?

1 A. Yes, sir.

2 Q. Will we hear from any of them in this trial?

3 A. Yes. The jury will hear from Dr. Bob Short.

4 Q. All right. So, Mr. Munger, I would like for
5 us to hear more about your invention and how the long
6 process of your -- your managing to invent it with your
7 team, but let's find out a little bit more about you
8 first.

9 Where do you live?

10 A. I live in Crownsville, Maryland, which is just
11 outside of Annapolis, Maryland.

12 Q. Are you married?

13 A. Yes, sir.

14 Q. Did you go to college?

15 A. Yes, sir.

16 Q. Where did you attend college?

17 A. I attended the United States Naval Academy and
18 then later MIT.

19 Q. Why did you choose to attend the Naval
20 Academy?

21 A. Well, my great-grand -- great-great
22 grandfather was a fisherman out of Maine, and my dad
23 commanded destroyers during World War II, so I guess
24 it's pretty much in my blood.

25 Q. When did you graduate from the Naval Academy?

1 A. 1967.

2 Q. What did you do then?

3 A. I was commissioned as a -- an officer at the
4 rank of ensign and went off to my first duty station,
5 which was a destroyer off Vietnam.

6 Q. What were your duties on that destroyer off
7 the coast of Vietnam?

8 A. I was a gunnery assistant.

9 Q. Would you say that your duties as a gunnery
10 assistant were technical?

11 A. Yes, sir. I was responsible for the radar,
12 the alignment of the guns, the computers that -- that
13 operated the guns, yes, sir.

14 Q. Okay. And what -- what's the next duty you
15 had after that ship?

16 A. I went to another destroyer where I was the
17 weapons officer and became responsible for all of the
18 weapon systems on the ship.

19 Q. And what about after them?

20 A. After that, I became the commanding officer of
21 a mine sweeper, and then went to MIT.

22 Q. Okay. So you were the commanding officer of
23 your own ship?

24 A. Yes, sir.

25 Q. At what age?

1 A. 28.

2 Q. Now, you said then you went to MIT.

3 Is that the Massachusetts Institute of
4 Technology?

5 A. Yes, sir.

6 Q. Were you still in the Navy when you went to
7 MIT?

8 A. Yes, sir.

9 Q. How did that come about?

10 A. Well, the Navy sends certain of its officers
11 to engineering school so that they can work on the
12 technology in the Navy and ships.

13 Q. What did you study during your time at MIT?

14 A. I studied naval architecture and marine
15 engineering.

16 Q. Now, when you were studying those subjects --
17 and I guess we're talking about the mid-'70s; is that
18 right?

19 A. Yes, sir.

20 Q. Did you use computers?

21 A. Yes, sir.

22 Q. What did you have reason to use computers for
23 at MIT?

24 A. Well, for -- to get a master's, you needed to
25 do research and write a thesis. And my -- my research

1 was the development of a -- of a program for ship design
2 that if you modified the dimensions of the ship, it
3 would tell you how it would change performance.

4 Q. So did you write that computer software?

5 A. Yes, sir.

6 Q. Now, just looking around the courtroom, I
7 guess I could pick out a dozen computers very easily,
8 but this is the mid-'70s we're talking about.

9 What were computers like then?

10 A. Well, it was -- it was early in the use of
11 computers for engineering computations, and a computer
12 was in a room that was this size. And if you wanted to
13 write a program, you had to type it out on punch cards,
14 put all the punch cards in a box, and take it to the
15 room that had the big computer in it. They would run
16 it. You would come back in a few hours, and they would
17 give you a printout, and you'd go through this process
18 over and over.

19 Q. Now, did you -- were you still on active duty
20 in the Navy throughout your time at MIT?

21 A. I was.

22 Q. And you were at MIT for four years; is that
23 right?

24 A. Three -- three years, sir.

25 Q. Three years.

1 And did you get a degree from MIT?

2 A. Yes, sir.

3 Q. What was that?

4 A. I got a master's in naval architecture, marine
5 engineering, and an engineer's degree called naval
6 architect.

7 Q. And after you got those graduate degrees from
8 MIT, what did you do then?

9 A. I went back to sea with the Amphibious Forces,
10 which are part of the Navy that work with the Marine
11 Corps. And then I returned to the Naval Academy and
12 taught engineering for two years.

13 And then I went back to a destroyer as second
14 in command, and then I went to Washington to work on
15 advanced ship concepts.

16 Q. What do you mean advanced ship concepts?

17 A. One of the projects I worked on was a stealth
18 ship that was -- could resist attack by cruise missiles.

19 Q. All right. During this second half of your
20 career as a naval officer after you left MIT, would
21 you -- were you involved with technology in the Navy?

22 A. Yes, sir.

23 Q. And did you specifically work, as part of your
24 duties in the Navy, with technology related to
25 communications?

1 A. Yes, sir.

2 Q. Now, we've been talking about that a lot
3 already today, security.

4 What is security?

5 A. Security is the protection of any -- any
6 system, whether it's your home or a ship or aircraft or
7 a communication system like the internet.

8 Q. And why is security important in
9 communications?

10 A. Well, it's important that if we're going to
11 communicate and we want to keep certain information
12 private, that we use certain approaches. And also if we
13 want to control critical systems, we want to keep -- we
14 want to make sure that that's done safely.

15 Q. Now, Mr. Munger, did your work in the Navy
16 help you later in your career when you were faced with
17 some issues having to do with communication security?

18 A. Yes, sir.

19 Q. In fact, did your experience in the Navy help
20 you invent the technology in this case?

21 A. Yes, sir.

22 Q. When did you retire from the service?

23 A. I retired in 1987.

24 Q. What was your rank?

25 A. Commander.

1 Q. So you retired from the Navy in 1987. By my
2 arithmetic, you were 43 years old. You had spent your
3 entire adult life in the United States Navy.

4 What did you decide to do then?

5 A. I went to a company called Science
6 Applications International Corporation, or SAIC.

7 Q. Tell us a little bit about SAIC.

8 A. Well, it was founded in 1969 by a doctor in
9 physics, and his concept was to bring scientists and
10 engineers together to do research for the Department of
11 Defense and the government.

12 Q. So what -- what was the -- what was the charge
13 of SAIC?

14 A. SAIC was taking science and figuring out how
15 to apply it to present-day problems.

16 Q. How many employees were there at SAIC when you
17 joined?

18 A. When I joined, there were 6,000.

19 Q. 6,000?

20 Why did you make this decision to go to work
21 at SAIC?

22 A. There were two reasons. One, I had met in the
23 Navy some of the scientists and engineers that worked
24 there, and I had a lot of respect for them, and I wanted
25 to join and work with them.

1 The other one was it was an employee-owned
2 company, meaning that each of the engineers or employees
3 that worked at that company have ownership stake in the
4 company.

5 Q. All right. You say that most of SAIC's work
6 was for the governments in the realm of national
7 security.

8 Can you give us some examples of the kind of
9 things that SAIC has done for national security?

10 A. Well, a number of them are classified, but I
11 think one that we may touch on every day is the -- they
12 have developed sensors for airports to stop terrorists,
13 and screening trucks and containers that come into port,
14 that sort of thing.

15 And also, some of the projects that I worked
16 on like War Breaker and Global Hawk.

17 Q. Before we go into those projects, I want to --
18 I want to touch on an issue that you briefly just
19 mentioned, that many of SAIC's projects are classified.

20 Do you mean by that that they are classified
21 by law as government secrets?

22 A. Yes, sir.

23 Q. Are you allowed to talk about classified,
24 secret matters that you have worked on?

25 A. No, sir.

1 Q. Was the work that you did, though, on what
2 became the patents in this case, classified?

3 A. No, sir.

4 Q. So is that -- the reason that you're able to
5 testify about it today is because it was not a
6 classified project?

7 A. That's correct, sir.

8 Q. Now, you mentioned a word, or maybe it's two
9 words -- I'm not sure -- before I asked you those
10 questions, and it was War Breaker.

11 What was War Breaker?

12 A. War Breaker was a program that networked
13 together a lot of real-time simulators so they could be
14 evaluated, the different combat systems could be
15 evaluated in real-time.

16 And it was also used as an analysis for
17 critical -- critical problems that were being faced.

18 Q. So let's talk about critical problems.
19 Was there a particular critical problem at the time you
20 were working on the War Breaker project at SAIC that
21 commanded your attention?

22 A. Yes, sir.

23 Q. And -- and did this challenge that you
24 encountered at War Breaker turn out to be important to
25 the invention in this case?

1 A. Yes, sir.

2 Q. What -- what was that challenge?

3 A. The challenge was we were in the first Iraq
4 war, and the Iraqis were firing terrorists missiles into
5 Israel. These were called scuds, and they presented
6 some serious problems that -- we were having difficulty
7 encountering them.

8 Q. What -- what was the particular problem with
9 the scud missiles and their launchers?

10 A. Well, the -- the scud launcher is a truck, and
11 it could actually hide under tunnels or under bridges.
12 And it could come out and set up and fire and go back
13 into hiding in less than 10 minutes.

14 Q. Now, did this problem of scud missiles lead to
15 a new project for you and for SAIC?

16 A. Yes, sir, it did.

17 Q. What was that project called?

18 A. That project was called Global Hawk.

19 Q. What role did you play in the Global Hawk
20 project?

21 A. SAIC had a contract to provide system
22 engineering and the technical support to the program
23 office that was doing the development of this -- of this
24 system, and I was the program manager.

25 Q. Now, did the Global Hawk program introduce you

1 to some problems or issues that would later be important
2 to you and your team in coming up with the invention in
3 this case?

4 A. Yes, sir.

5 Q. Let's find out a little bit more about it.
6 What is Global Hawk?

7 A. I -- I did bring a picture, so I thought I'd
8 show it.

9 Q. Okay. Can you show us that picture?

10 A. It just came up.

11 So I'll tell you about it then?

12 Q. Yes, please.

13 A. This is a picture of the Global Hawk, and you
14 can't tell by looking at this picture, but this is a
15 very, very big aircraft. From tip of the wings is about
16 120 feet. So this is pretty large.

17 It's got no pilot, so this is what they call
18 an unmanned air vehicle, and it has sensors that can
19 see -- see the ground in very good resolution. And it
20 also flies very high. It flies at 60,000 feet.

21 And if you've taken a jet from Dallas to New
22 York, they fly about 30,000 feet. So this flies three
23 times higher than a commercial jet.

24 Q. Okay. Now, you mentioned that this is --

25 THE COURT: Excuse me, Mr. Cawley. Did

1 you say it has no power.

2 THE WITNESS: No pilot.

3 THE COURT: No pilot. Okay.

4 THE WITNESS: Nobody driving, sir.

5 THE COURT: I wasn't sure how it got up
6 there.

7 THE WITNESS: Sorry for my accent.

8 Q. (By Mr. Cawley) Let me pick up on that.

9 It had no pilot. You said it was an unmanned
10 aircraft?

11 A. Yes, sir.

12 Q. Well, didn't the military already have
13 unmanned aircraft? Sometimes we hear them called
14 drones?

15 A. Yes, sir.

16 Q. Well, why couldn't the military's drones solve
17 the scud problem?

18 A. Well, the problem that we had were these were
19 terrorist weapons, and they could come out anytime
20 during the day or night and shoot. And the low-flying
21 drones couldn't see very far, both sides, so it would
22 take a lot of them to cover them. And they really
23 couldn't stay up in the air.

24 This one could stay up in the air for 24
25 hours, and it could be replaced. So it was always up

1 there, and it could see a very far distance.

2 Q. Okay. Well, what about satellites?

3 Satellites are very high, and they stay up all
4 the time.

5 Why couldn't they see the scud missiles?

6 A. Well, they could. But a satellite also flies
7 over three or four times a day, depending on the type of
8 satellite. So there were still gaps when the enemy
9 could come out and attack.

10 Q. So how would the Global Hawk solve the problem
11 of scud missiles?

12 A. Well, it's probably easier for me to just show
13 you what the concept was.

14 Q. Please do.

15 A. So here -- here's the Global Hawk, and we sort
16 of knew the general area that these bad guys were going
17 to come out and shoot the rockets. So we would place
18 the -- the Global Hawk over there so it could watch this
19 area 24 hours a day.

20 We also needed to get the information very
21 quickly to the ground, because we didn't have a lot of
22 time. So there was a public commercial satellite that
23 was used. And when a picture was taken, it would beam
24 that picture through the satellite to an operator on the
25 ground.

1 So the concept here was that when one of these
2 scud launchers would come out -- and that's a picture of
3 the scud launcher in the bottom left-hand corner -- the
4 Global Hawk sensor would get a picture of it, and it
5 would very quickly be able to transmit it through the
6 satellite to an operator on the ground who had resources
7 that could be brought in.

8 And in this case, this is a picture of an
9 F-15. And he would send a message to the F-15, and the
10 F-15 could attack the missile launcher.

11 Q. Now, was there a particular issue about the
12 security of communications in this Global Hawk system?

13 A. Yes, sir.

14 Q. What was that?

15 A. Well, to my knowledge, it was one of the first
16 times that we were using commercial public
17 infrastructure for operating a critical military system.

18 Q. Okay. You said some words there I want to
19 make sure I understand.

20 Let me ask this question: How had the
21 military -- after all, this was being done for the
22 military, right?

23 A. Yes, sir.

24 Q. How had the military traditionally kept its
25 communications secure?

1 A. Well, they would -- they would build their
2 communication systems and own their own communication
3 systems, and they would build in whatever was necessary
4 encryption and hardness. And that was the practice up
5 until this time.

6 Q. How is Global Hawk different?

7 A. Well, Global Hawk was using a satellite that
8 other people could rent to relay TV or make network
9 connections between one facility and another facility in
10 two different countries.

11 Q. So you're telling us that there are satellites
12 orbiting over the Earth that are just owned by
13 businesses?

14 A. Yes, sir.

15 Q. And those -- their businesses could lease out
16 bandwidth or transmission capability of that satellite?

17 A. Yes, sir.

18 Q. So, for example, for anybody who has satellite
19 TV or may see those dishes in people's yards, that's
20 coming from some satellite that a business owns; is that
21 right?

22 A. That's correct.

23 Q. So are you telling us that the military that
24 made the decision, rather than to use its own
25 satellites, to simply lease or rent space on a

1 commercial or public satellite?

2 A. That's correct.

3 Q. Why did they do that?

4 A. Well, the picture sizes and the radar image
5 sizes were very large, and it would have really taxed
6 the military-owned systems. So it was the first time we
7 really started moving lots and lots of information very
8 quickly.

9 Q. Now, did the military's decision to use a
10 commercial satellite create any particular security
11 issues?

12 A. Yes, sir.

13 Q. Tell us about that.

14 A. Well, we sure didn't want any of this to be
15 intercepted. And so measures were taken to make sure
16 that all of the transmissions were very secure.

17 Q. Was Global Hawk a success?

18 A. Yes, sir.

19 Q. Did it take down scud missiles?

20 A. No, sir. The Iraq war was over by the time
21 the first ones were in the air.

22 Q. Where is it being used?

23 A. It's not -- it's being used today in both Iraq
24 and Afghanistan.

25 Q. Who at SAIC worked on this Global Hawk project

1 with you?

2 A. We had a number of engineers, but Dr. Bob
3 Short and Dr. Vic Larson also worked on this project.

4 Q. Now, Mr. Munger, did Global Hawk, this project
5 you've just described to us, even after the project was
6 finished, influence your thinking about future security
7 issues?

8 A. Yes, sir.

9 Q. Tell us about that.

10 A. Well, there are two aspects. It -- it became
11 clear to me that we were really going to have to move
12 information around the battlefield very quickly and very
13 securely. And there are battles that could be anywhere.
14 I mean, we couldn't have projected that we were going to
15 be in Afghanistan.

16 So what I realized that the internet was going
17 to need to become an asset for the security of the
18 nation, and that was going to take some really good
19 secure technology for doing it.

20 The other -- the second part of this was that
21 business was being conducted over the internet more and
22 more every day. It was just the beginning. We were
23 buying books at Amazon, but it also meant that we were
24 going to -- we really needed to make the internet safe
25 for business, because it was going to be important to

1 the nation.

2 Q. So what did you do in response to your
3 thinking about these future security issues?

4 A. The first thing I did was I went and talked to
5 my -- my management all the way up to the CEO, and I
6 asked them if we could put together a small team to take
7 a look at this problem, and they agreed. They broke a
8 few of us loose to work on it.

9 And the other thing was that I wrote a -- I
10 wrote a paper called Aladdin.

11 Q. Okay. Let's -- let me show you Plaintiff's
12 Exhibit 365.

13 Is this a copy of the paper that you wrote?

14 A. Yes, sir.

15 Q. And you see the title up there at the top,
16 Aladdin? Do you see that?

17 A. Yes, sir, I see that.

18 Q. Why did you call the paper Aladdin?

19 A. Well, the concept that was presented in the
20 paper is we wanted to be able to bring the right people
21 together very quickly to make decisions in support of
22 military operations.

23 And the idea was that you wanted to make it so
24 easy that you could rub Aladdin's lamp and the genie
25 would make everything connect, and so the soldier would

1 get the support that he needs.

2 Q. So who read the Aladdin paper?

3 A. The Aladdin paper was distributed in DARPA.
4 It was provided to other engineers and scientists in the
5 company, and some of them provided it to their sponsors
6 like the Army.

7 Q. The United States Army?

8 A. Yes, sir.

9 Q. Now, you mentioned something that I want to --
10 I want to make sure we understand what you were
11 referring to, because I think it may come up again.
12 You said DARPA. What is DARPA?

13 A. DARPA is the Defense Advance Research Project
14 Agency.

15 Q. All right. So did the efforts that you were
16 making, the small group that you had assembled within
17 SAIC, and this Aladdin paper, did this lead to the
18 project that eventually produced the invention in this
19 case?

20 A. Yes, sir, it did.

21 Q. Who was that project for?

22 A. That project was for a company called
23 In-Q-Tel.

24 Q. What is In-Q-Tel?

25 A. In-Q-Tel was a company formed by Congress to

1 invest in very early, promising technology that would
2 have application both commercially and would help the
3 CIA.

4 Q. The Central Intelligence Agency?

5 A. Yes, sir.

6 Q. Why wouldn't the CIA just do it themselves?

7 A. Well, if -- if it also -- if the technology
8 was useful to the CIA and also had commercial
9 application, it would be -- it would cost less to
10 provide that capability to the CIA than if they had to
11 develop and maintain it in-house.

12 Q. So are you saying that this was a way of
13 farming out to private enterprise the development of
14 technology that the CIA might want to use without having
15 to spend a lot of government money to do it?

16 A. Yes, sir.

17 Q. Why are companies like yours, your company
18 back then, SAIC, interested in working with In-Q-Tel?

19 A. There were -- there were two aspects. One,
20 we -- we were getting funded to do the research, which
21 was the model for SAIC. And, two, we were also allowed
22 to keep the invention rights.

23 Q. And what did the CIA get?

24 A. Well, the CIA got the -- got to test and to
25 utilize on a limited basis anything that was developed.

1 Q. So did the C -- did your company, SAIC, get a
2 contract with this congressionally set up company,
3 In-Q-Tel to pursue your ideas?

4 A. I'm sorry. Would you repeat the question?

5 Q. Sure.

6 Did your company, SAIC, get a contract with
7 In-Q-Tel to pursue your ideas for the CIA?

8 A. Yes, sir.

9 Q. Let me show you Plaintiff's Exhibit 311.
10 Is that a copy of the contract between your company and
11 In-Q-Tel?

12 A. Yes, sir.

13 Q. I see at the very top there it actually says
14 In-Q-IT.

15 Why is that?

16 A. They went through a name change.

17 Q. Okay. So is this -- even though it says
18 In-Q-IT, this is still the same company, In-Q-Tel, set
19 up by Congress?

20 A. Yes, sir.

21 Q. What was the project that was -- this contract
22 was for?

23 A. Well, we had proposed to them survivable VPN.
24 But the concept was they were interested in having their
25 agents be able to connect and use the internet to -- to

1 very privately connect back to resources that might help
2 their agents.

3 Q. Well, surely the CIA has its own
4 communications equipment.

5 Why did they need to be able to use the
6 internet?

7 A. Well, they -- they -- they have a lot of
8 communication capabilities themselves, but this would
9 have been a complement, and the internet was becoming
10 used more and more all over the world.

11 Q. And was the potential use of the internet by
12 agents of the CIA similar to the issues that you faced
13 in Global Hawk and wrote about in the Aladdin paper?

14 A. Yes, sir.

15 Q. What was the amount of the contract that SAIC
16 entered into with In-Q-Tel?

17 A. It was approximately \$3-1/2 million.

18 Q. Now, at the time you undertook this project,
19 did you assemble a team of people to work with you?

20 A. Yes, sir.

21 Q. And were you and your team already familiar
22 with some ways to make internet communications more
23 secure?

24 A. Yes, sir.

25 Q. So -- so some -- some ways to make internet

1 communication secured already existed at the time you
2 started on this project.

3 Is that what you're telling us?

4 A. Yes, sir.

5 Q. For example, didn't online companies that were
6 selling things -- I think you mentioned Amazon -- didn't
7 they have security?

8 A. Yes, sir, they did.

9 Q. What was it called?

10 A. It was called https.

11 Q. What does https stand for?

12 A. Hypertext transport protocol secure.

13 Q. So why wouldn't that kind of security have
14 worked for the CIA?

15 A. Well, it was basically a point-to-point
16 communication to a server. And they wanted the
17 flexibility to be able to reach various computers on --
18 on the fly.

19 Q. Could you do that with https?

20 A. No, sir.

21 Q. Were there other ways that were available at
22 this time to secure limit on the internet?

23 A. Yes, sir.

24 Q. What was that?

25 A. Virtual private network.

1 Q. We have already heard some about that, but I
2 guess you're the first witness to tell us about it.

3 What is a virtual private network?

4 A. Well, I -- it's probably easiest to take the
5 three words. There's virtual, private, and network. So
6 I'm going to look backwards, because it's easier for me.
7 If we start with network -- we saw some pictures -- but
8 if we think about two computers with a wire between it
9 that has the capability to transfer files or voice or
10 stream video, those two -- those two computers are
11 networked together.

12 If I put a third computer up and put a wire
13 between them and I can now transfer information between
14 all three, that's a network, and you could keep adding
15 computers. So that's what a network is in very simple
16 terms.

17 So then we're going to go to private. We had
18 virtual private network, so private is -- if I have
19 those three computers in my house with the door locked
20 and somebody would have to come in and tap the wire,
21 because I've got -- it's in my house -- that's called
22 private. And it would be difficult for somebody to see
23 the traffic between those three computers.

24 So virtual means that it's going to have the
25 same sort of levels of -- of -- of safety and privacy,

1 except that if I had a computer out over the internet --
2 and we've already heard that you can hear things; people
3 can hear traffic over the internet -- but if I secure
4 that with something that encrypts the traffic and makes
5 it safe, that's now become the virtual private network.

6 So those -- that's my easy definition, sir.

7 Q. Okay. Well, besides your easy definition,
8 you're aware that Judge Davis has defined for us all
9 what a virtual private network means in your patent,
10 aren't you?

11 A. Yes, sir.

12 Q. Remind us -- we'll take a look at what Judge
13 Davis has told us the meaning of virtual private network
14 as it's used in the patent.

15 Can you read that to us?

16 A. Yes, sir.

17 A network of computers, which privately
18 communicate with each other by encrypting traffic on
19 insecure communication paths between the computers.

20 Q. Thank you, sir.

21 Now, Mr. Munger, you didn't invent virtual
22 private networks, did you?

23 A. No, sir.

24 Q. What did you and your team invent?

25 A. We invented an easy way to automate their

1 set-up.

2 Q. Did your team consider virtual private
3 networks as a possible solution for the In-Q-Tel and CIA
4 project?

5 A. Yes, sir. It was promising.

6 Q. Did your team look at and study a variety of
7 software and hardware that was available in the late
8 1990s to set up or create VPNs?

9 A. Yes, sir.

10 Q. For example, did your team look at some
11 software that Microsoft offered at that time which would
12 set up a VPN?

13 A. Yes, sir.

14 Q. Did you look at the software of other
15 companies that could be used at that time to set up a
16 VPN?

17 A. Yes, sir.

18 Q. Were there some hardware products that could
19 also be used to set up a VPN?

20 A. Yes, sir.

21 Q. Did you find that there were any problems with
22 these products that you and your team studied?

23 A. Yes, sir.

24 Q. What was it?

25 A. The biggest problem was the complexity in --

1 in the number of steps that it took to get to the -- to
2 VPNs to communicate.

3 Q. Can you give us an example?

4 A. You might have to type in as many as 15
5 different settings and make sure they were all correct
6 before the VPN would work.

7 Q. Did -- your team at SAIC, which included
8 Ph.D.s in this field, as well as other people who are
9 highly expert, did they have trouble setting up VPNs
10 with the available software?

11 A. Yes, sir.

12 Q. And do you understand that Dr. Short, who is
13 not in the courtroom anymore but will be later, will be
14 able to actually demonstrate what was required to set up
15 a VPN back in this time period?

16 A. Yes, sir, he will.

17 Q. Did you think that these products that were
18 available were appropriate solutions for what the CIA
19 needed?

20 A. No, sir.

21 Q. So how long did your team wrestle with this
22 problem of the undue difficulty and complexity of
23 setting up virtual private networks?

24 A. I would estimate four or five months.

25 Q. What did you feel that you needed to

1 accomplish to solve that problem?

2 A. Well -- well, we really wanted it to become as
3 easy as making a telephone call. We wanted it so easy
4 anybody could use it, and that it pretty much happened
5 in a few seconds or so.

6 Q. Okay. So you had realized, as you were
7 struggling with this problem, you and your team, that
8 you wanted to make it easy.

9 But was it easy to make, creating a VPN
10 simple?

11 A. No, sir.

12 Q. But did your team working on this issue
13 eventually have a breakthrough that solved the problem?

14 A. Yes, sir.

15 Q. How did it happen?

16 A. It was in September of 1999, and we were
17 visiting a professor up at Columbia University in New
18 York, that had been working on making phone calls over
19 the internet.

20 And on the train ride back, we were talking
21 about -- this is Dr. Bob Short, myself, Dr. Vic Larson.
22 We were on a train ride back from New York to the
23 Washington area, and we were talking about how we wanted
24 it to be as -- as an example, as simple as people
25 understanding how to make a phone call.

1 And Dr. Short said -- came up with the idea.
2 I mean, it was startling. He said, well, how do we make
3 a phone call, or how do we make a connection on the
4 internet? And his -- his a-ha at the time was that
5 people that used the internet knew -- could remember how
6 to go to Amazon.com or eBay.com, which is entering a
7 domain name.

8 And what he realized was that if we could make
9 people, or a piece of software that was entering a
10 domain name and doing look-up, automatically trigger the
11 virtual private network that we had a way forward.

12 Q. How did you feel when he made that suggestion,
13 when he got that idea?

14 A. Well, I mean, we've all struggled with
15 problems. We think about them over a very long time,
16 and you don't feel like you're making a lot of progress.
17 You have the goal; you kind of know what you'd like to
18 achieve.

19 But when he said it, it was kind of like, wow,
20 I mean, this is it. This is -- this is a way to focus
21 how we could possibly pull this off.

22 Q. Now, even after Dr. Short had this idea on
23 that train ride, did you still have work to do?

24 A. Oh, yes, sir.

25 Q. How long did it take between that breakthrough

1 idea and the time that you had the details of the
2 invention worked out?

3 A. I'd probably say three or four months.

4 Q. Okay. Let me show you Plaintiff's
5 Exhibit 367.

6 What is this document?

7 A. This is a progress meeting with a company that
8 we talked about before, In-Q-Tel, and we -- we named our
9 technology. I mean, it went through a lot of names.
10 You've heard NetEraser and all sorts of things.

11 But at this time, we were calling it In-Q-Net
12 in honor of our research sponsor. And in this
13 presentation are the first presentation of the ideas of
14 that automation.

15 Q. So are there a lot of ideas in this
16 presentation?

17 A. Yes, sir.

18 Q. Had nothing to do with your invention?

19 A. That's correct.

20 Q. But is this the first document you know of in
21 which the idea for your invention was presented?

22 A. Yes, sir.

23 Q. And that was in January of the year 2000?

24 A. Yes, sir.

25 Q. After your invention, how long does it take a

1 user to set up a virtual private network?

2 A. A few seconds.

3 Q. And will Dr. Short actually be able to show us
4 that in the courtroom?

5 A. Yes, sir.

6 Q. And who would use your invention to set up
7 secure internet communications?

8 A. As I mentioned before, basically anybody. Any
9 individual that wanted to connect with any other
10 individual or their company or small businesses. Pretty
11 much anybody could use it, sir.

12 Q. So did you file for patents on your invention?

13 A. Yes, sir.

14 Q. And as part of your employment agreement with
15 SAIC, did you and your co-inventors agree that you would
16 transfer your patent rights to SAIC?

17 A. Yes, sir.

18 Q. Let me show you Plaintiff's Exhibit 9 just
19 quickly.

20 Is this some documents filed with the Patent &
21 Trademark Office that contained the assignments of the
22 application that eventually became the '135 patent?

23 A. Yes, sir.

24 Q. And the same question with regard to
25 Plaintiff's Exhibit 7.

1 Is that a document filed with the U.S. Patent
2 & Trademark Office that contains the assignment from you
3 and your co-inventors of the application that became the
4 '180 patent to SAIC?

5 A. It is.

6 Q. What role did you play, Mr. Munger, in
7 applying for the patents?

8 A. I worked with the patent attorneys in helping
9 to draft the specifications and reviewing the patent,
10 sir.

11 Q. And let me show you Plaintiff's Exhibit 2.

12 Is this the document that is something called
13 the file history; that's the whole record of the
14 communications back and forth with the Patent Office?

15 A. Yes, sir.

16 Q. And is Plaintiff's Exhibit 5 the same thing
17 for the second patent?

18 A. Yes, sir.

19 Q. Let's take a look at Plaintiff's Exhibit 3.
20 Do you recognize that document?

21 A. Yes, sir.

22 Q. What is it?

23 A. That's what we call the '135 patent, sir.

24 Q. When did the '135 patent issue? When did the
25 Patent Office actually approve and issue that patent?

1 A. That was in December of 2002.

2 Q. So, Mr. Munger, how did you feel when you got
3 that first patent?

4 A. Well, I was pretty excited. It was my first
5 patent, and -- I don't know. We always grow up hearing
6 about Ben Franklin and Thomas Edison and Alexander
7 Graham Bell. It was an interesting feeling to become a
8 member of that club.

9 Q. And let me ask you to look at Plaintiff's
10 Exhibit 6.

11 What's that document?

12 A. This is what we call the '180 patent.

13 Q. This is your second patent that was approved
14 and issued by the United States --

15 A. Yes.

16 Q. -- Patent Office?

17 Did you continue during this time, Mr. Munger,
18 to work on software to deliver to In-Q-Tel?

19 A. Yes, sir.

20 Q. What -- what did you call that software?

21 A. NetEraser.

22 Q. Why did you give it that name?

23 A. One of the primary things that we were working
24 on with them was a different technology called address
25 hopping. And the goal of that software was -- of that

1 technology was to mask the existence of the
2 communication on the internet.

3 Q. So did you deliver prototype software --
4 NetEraser software to In-Q-Tel and to the CIA?

5 A. Yes, sir.

6 Q. Did the CIA use it?

7 A. I -- they tested it, but I can't tell whether
8 they used it, sir.

9 Q. Well, how is it that you don't know if they
10 used it or not?

11 A. Their communication technologies are very
12 secret, and I -- I -- I didn't have the need to know
13 about it, sir.

14 Q. Now, at this time, in -- in 1999 and 2000,
15 you've recently finished the NetEraser project.

16 Did you think that your invention and your
17 team's invention was ahead of its time?

18 A. Yes, sir.

19 Q. Why do you say that?

20 A. Well, at the time, I was using a computer at
21 home, and it worked. But we were using a dial-up
22 connection, which was very slow. And where we saw the
23 promise of this was in -- in voice and in screening
24 video.

25 And though in my research I was lucky enough

1 to work with very high capable networks, it was
2 really -- it was going to take time before households
3 got the large bandwidth which would demand this type of
4 security.

5 Q. But even though you had that feeling that your
6 invention might be a little ahead of its time, was your
7 company, SAIC, free to try to do something with the
8 invention?

9 A. Yes, sir.

10 Q. Did you ask any others to help evaluate the
11 work and prospects for your invention?

12 A. We did.

13 Q. Who did you talk to?

14 A. One of the ones that I worked with and
15 provided support to was Cambridge Strategic Management
16 Group.

17 Q. What is Cambridge Strategic Management?

18 A. It was a consulting firm that the company
19 hired to take a look at the technology and -- and its
20 market viability.

21 Q. Okay. What did Cambridge conclude?

22 A. They concluded -- we had them both look at the
23 whole body of technology. But they concluded that the
24 automation was the most promising commercially.

25 Q. Let's look at Plaintiff's Exhibit 359.

1 Is this the presentation that was given to
2 your company, SAIC, by Cambridge?

3 A. Yes, sir.

4 Q. And if we look at Page 3 of that presentation,
5 what did Cambridge have to say about your automation
6 invention?

7 A. Well, they said that we had patented
8 technology that allows -- that could play a significant
9 role in providing hassle-free VPN connections and
10 enhanced security.

11 Q. Okay. And did they also attempt at least to
12 place some kind of value on what this technology might
13 be worth?

14 A. Yes, sir.

15 Q. Let's look at the next page.
16 What do they say?

17 A. Well, they said that a net present value,
18 which is what is it worth, if it was a lump sum today,
19 would be approximately \$190 million.

20 Q. Now, Mr. Munger, have you seen various
21 estimations for what this technology might be worth over
22 the years, high and low?

23 A. Yes, sir. And they're all over the place.
24 The only thing that this said to me was that -- that it
25 was a promising technology.

1 Q. Okay. So what did you do then?

2 A. The company had -- we were coming to the end
3 of In-Q-Tel's contract, and the company decided that
4 they might want to attempt to roll the technology out
5 into a company and seek investment.

6 Q. Why did they need money from investors?

7 A. Our technology was still in prototype form.
8 It wasn't ready to go out to the market. It wasn't --
9 it still required development.

10 Q. So why didn't SAIC just do that themselves?

11 A. It's not their culture to try to set up and
12 run themselves a commercial -- a commercial company.
13 They're a company that sells engineers for hours plus
14 fee, sir.

15 Q. Well, what kind of companies did you go talk
16 to, to try to raise money for your invention?

17 A. We talked to venture capitalists.

18 Q. What is a venture capitalist?

19 A. Well, a venture capitalist is an investor that
20 is looking for brand new companies, early start, that
21 possibly have very high pay-off. So they're usually
22 willing to take more risks, and they expect that if the
23 company does well, they're going to make more money on
24 their investment, sir.

25 Q. And are there venture capitalists, for

1 example, in investing in technology start-up companies.

2 A. There are, sir.

3 Q. Now, what -- what time period are we talking
4 about that you went out on the road to talk to venture
5 capitalists about the possibility of investing in your
6 invention?

7 A. This was springtime, 2001.

8 Q. Spring of 2001, was this a good time to be out
9 looking for money for a high-tech start-up company?

10 A. It was the worst time.

11 Q. Why do you say that?

12 A. Well, we're in a recession now. But in 2001,
13 we were right in the middle of what was called the
14 dot.com bust. And it particularly hit hard on
15 technology companies.

16 So investment in new ventures was very hard to
17 find.

18 Q. So how many companies did you talk to, to try
19 and raise money for your invention?

20 A. Approximately 30.

21 Q. 30?

22 A. Yes, sir.

23 Q. Let me show you Defendant's Exhibit 3192.

24 What's this?

25 A. This is a memo from Mr. Ed Hendrick, who works

1 in the SAIC Commercialization Group, to our SAIC CEO,
2 giving him the status of our investment search.

3 Q. Okay. If we could see Page 2 of that
4 document, does this page list some of the potential
5 venture capital companies that you talked to about the
6 possibility of raising money?

7 A. Yes, sir.

8 Q. The second page -- or I guess, the third page,
9 more?

10 A. Yes, sir.

11 Q. Then the one after that?

12 A. Yes, sir.

13 Q. How many are on the list in total?

14 A. I think when I counted, I believe there's 30
15 on that list, sir.

16 Q. And where were they located?

17 A. Some of them were in the Silicon Valley just
18 south of San Francisco, some in New York. And there's
19 probably a couple spread around in other major cities,
20 sir.

21 Q. Okay. Did any of these companies invest in --
22 in your invention?

23 A. No, sir.

24 Q. Why did you -- why do you think you couldn't
25 find investors at that time?

1 A. Well, there was the tightness of funds, but
2 also most of these companies that we talked about were
3 trying to prop up their companies that they had present
4 investments in. And they also were looking, if they had
5 new money to invest, in, one, companies that are very
6 close were already going out to their first customers
7 and ready to -- to make money, sir.

8 Q. Were you ready to go out to your first
9 customers for your invention?

10 A. No, sir. We needed seed funds to mature our
11 product, sir.

12 Q. When you mature your product, what does that
13 mean?

14 A. Well, we had a prototype, and we needed to
15 develop it into a product. And it was just in beta, and
16 until it's ready to take the first customers for test
17 and evaluation, sir.

18 Q. In addition to these venture capital
19 companies, did you also talk to some companies about the
20 possibility of going into a development agreement with
21 you so that you could develop your invention, bring it
22 to maturity together?

23 A. Yes, sir.

24 Q. Who did you talk to about the possibility of
25 doing that?

1 A. We talked to Morgan Stanley. We talked to
2 eBay. We talked to Amazon.com.

3 Q. And what did you propose to those companies?

4 A. Well, again, we were looking for development
5 dollars. And part of that discussion was on a -- some
6 of our other technology for robust VPNs.

7 Q. And did any of those companies agree to
8 co-develop your invention with you?

9 A. No, sir.

10 Q. Why did you think you couldn't find a company
11 at that time that was willing to co-develop your
12 invention?

13 A. I think those companies are used to buying
14 things -- off-the-shelf-solutions that are all ready to
15 go, sir.

16 Q. Did you have a product on the shelf ready to
17 go?

18 A. No, sir.

19 Q. Now, you told us that you spent a lot of time
20 on the road in this time period, trying to find
21 investors for your invention.

22 Did others -- people back at the shop keep on
23 working on the software for the invention?

24 A. Yes, sir, they did.

25 Q. But did the company, SAIC, eventually decide

1 that it had to stop the development of your invention?

2 A. Yes, sir.

3 Q. Why -- why did that happen?

4 A. Well, it was clear that we were not going to
5 get investment, and they decided to shut down the
6 commercialization effort and allow the technical team --
7 there was a budget, and there was some money left in
8 it -- they allowed the technical team to continue
9 development on the prototype to where it became -- to
10 where it became a beta.

11 Q. When did SAIC decide that it would no longer
12 put new funds into the development?

13 A. June of 2001.

14 Q. And what was the plan?

15 A. The plan was to continue with the remaining
16 funds to develop the product and also return to
17 government customers, which was something that SAIC is
18 used to, and see if we could possibly interest them in
19 continuing the development effort.

20 Q. Okay. Let me take out a couple of minutes
21 there to ask you about something we heard about this
22 morning, this company called Aventail.

23 Did SAIC own a company called ANX?

24 A. Yes, sir.

25 Q. What business was ANX in?

1 A. They were in the business of connecting parts
2 vendors for the automobile industry to automobile
3 manufacturers.

4 Q. And did ANX have a need for secure
5 communications?

6 A. Yes, sir.

7 Q. So what product did they choose to accomplish
8 that?

9 A. Aventail.

10 Q. Why didn't they choose your invention?

11 MR. POWERS: Objection, Your Honor.
12 That's calling for speculation at least for ANX's
13 decision for which Mr. Munger he can't --

14 THE COURT: Restate your question.

15 Q. (By Mr. Cawley) Why do you think that they
16 chose something other than your invention?

17 MR. POWERS: Same objection.

18 THE COURT: Objection is sustained.

19 Q. (By Mr. Cawley) Did SAIC also invest money in
20 Aventail?

21 A. Yes, sir.

22 Q. When was that?

23 A. I believe the fall of 2001.

24 Q. Do you know why SAIC decided not to continue
25 to invest money in your invention?

1 A. No, sir.

2 Q. Did you continue working on the beta?

3 A. Yes, sir.

4 Q. And how was progress going in the late summer
5 of 2001?

6 A. It was going well.

7 Q. Let me show you Plaintiff's Exhibit 94.
8 What is this document?

9 A. This is an e-mail from Dr. Bob Short to
10 Mr. Don Foley, who was one of the upper managers in
11 SAIC.

12 Q. And what does he tell him about the progress
13 on the beta version of your invention?

14 A. Well, he says that he thought people would be
15 surprised and pleased with the beta product that is
16 coming out of this final push.

17 Q. Okay. You know what? I apologize. We've
18 been using this word beta several times now.

19 What is a beta?

20 A. A beta is a -- is a product that is not quite
21 ready for full distribution out in the market. But it's
22 generally ready to have a community outside the company
23 or outside the developers test and evaluate it and give
24 it feedback, so you can harden it up so you're ready for
25 release.

1 Q. So what was Mr. Short telling us about the
2 progress on the beta on August 22nd, 2001?

3 A. Well, he thought it was going very well, sir.

4 Q. Did anything happen shortly thereafter which
5 made it more difficult for you and some other members of
6 your team to spend time trying to find a way to make
7 your invention successful?

8 A. Yes, sir.

9 Q. What was that?

10 A. On September 11th, the Twin Towers were
11 attacked.

12 Q. And what effect did that have on you and your
13 company?

14 A. Well, I think probably everybody in this room
15 knows where they were on that day, and shortly after
16 myself and others on the team really started looking for
17 ways that we might be able to prevent future attacks by
18 terrorists.

19 Q. Did you yourself launch a program for that
20 purpose?

21 A. Yes, sir.

22 Q. Tell us about that.

23 A. Well, we thought that data, the collection of
24 all materials, information -- all information about
25 terrorist activity is that we might be able, through

1 data mining and software, connect the dots and get
2 indications and warnings that might prevent future
3 attacks, sir.

4 Q. When did that project get off the ground?

5 A. We got it started in the November/December
6 timeframe of 2001.

7 Q. And how did it affect your work schedule?

8 A. Well, this was for the FBI. And in January,
9 Dr. Vic Larson and myself went full time in the FBI
10 headquarters to integrated prototype using these
11 concepts, sir.

12 Q. And how long were you located full time in the
13 FBI headquarters working on this anti-terrorism project?

14 A. About a year.

15 Q. Was that project a success?

16 A. Yes, sir.

17 Q. Now, did your -- the time that you devoted to
18 that project distract you from working on
19 commercializing your invention?

20 A. Yes, sir. There was some activity, but it
21 definitely put it on the back burner.

22 Q. You say it put it on the back burner, but even
23 though it was on the back burner, was it part of your
24 job to continue to work on finding an interest in your
25 invention, if you could?

1 A. Yes, sir.

2 Q. And did you have some success around that time
3 period?

4 A. Well, in the summer of 2002, we -- we got
5 interest from SafeNet.

6 Q. Who is -- or what is SafeNet?

7 A. Well, SafeNet is a company that developed VPN
8 clients. That's one of the things they did, which what
9 we were interested -- we actually used their product and
10 automated it in one of our early prototypes, so we had a
11 relationship with them. They're very well respected in
12 the security area. So we talked to them about licensing
13 our technology, sir.

14 Q. And did they enter into a license for your
15 technology?

16 A. Yes, sir.

17 Q. Let me show you Plaintiff's Exhibit 134. Is
18 that a copy of the technology license agreement between
19 Science Applications International Corporation and
20 SafeNet?

21 A. Yes, sir.

22 Q. What degree -- what rate or amount did SafeNet
23 agree to pay in this agreement?

24 A. 20 percent.

25 Q. Was there a cap on that amount?

1 A. No, sir.

2 Q. What was your team's reaction to the entry
3 into this agreement?

4 A. We were pretty excited.

5 Q. Well, what happened then?

6 A. SafeNet and -- and I was part of this; I
7 supported them a little bit in this -- talked to --
8 talked to some other customers, made some contacts
9 and -- but they couldn't get the interest that they
10 wanted.

11 Q. Okay. Were they going to be required to spend
12 money to develop your invention into a working product?

13 A. Yes, sir.

14 Q. And did they decide that they weren't willing
15 to do that?

16 A. That's correct, sir.

17 Q. Let me show you Plaintiff's Exhibit 344. What
18 is this document?

19 A. This is a letter to a Mr. Hendrick, who, as I
20 think I mentioned before, he's in our commercialization
21 group. And they hoped that managed service markets
22 would be favorable and would -- but they hadn't been
23 able to rationalize the capital expenditures to
24 commercialize the product and market the potential.

25 Q. What was the reaction to this letter back at

1 SAIC?

2 A. Yes, sir. Well, the other thing this letter
3 did was return our IP and cancel the license, and we
4 were very disappointed.

5 Q. Okay. Now, around this same time, though, Mr.
6 Munger, did you meet someone who did believe that they
7 could help make a success of your invention?

8 A. Yes, sir. One of the people that SafeNet
9 introduced me to was Mr. Kendall Larsen.

10 Q. Now you've already told us about Dr. Vic
11 Larson, one of the inventors. Is Kendall Larsen related
12 to him in some way?

13 A. No, sir. They're not related at all.

14 Q. So what did Mr. Larsen do?

15 A. Mr. Larsen was very excited about the
16 technology. And in 2004-2005, he approached SAIC,
17 raised some money, and started VirnetX, sir.

18 Q. How did he raise money for -- to start the
19 company, VirnetX?

20 A. He went out to friends and family, and there
21 was an investment bank that also located some matching
22 funds.

23 Q. Now, just to avoid confusion, did you actually
24 think of the name VirnetX?

25 A. Yes, sir.

1 Q. And was that a name you were using within SAIC
2 to describe the work on your invention?

3 A. Yes, sir. In the spring of 2001, that effort,
4 this organization was called VirnetX.

5 Q. So did SAIC agree to let Mr. Larsen name his
6 company VirnetX when he formed it?

7 A. Yes, sir.

8 Q. What was the relationship between SAIC and
9 VirnetX?

10 A. Well, there was a license arrangement that
11 could lead to the transfer of the patent, and also we --
12 we could -- we were going to provide some technical
13 support.

14 Q. Technical support to do what?

15 A. The technical support was -- it had been
16 awhile since 2001. This is the end of 2005. So we
17 wanted the inventors to come back together, take a look
18 at any changes to the network situation and technology,
19 and propose to him how to go forward to develop a
20 product.

21 Q. And did you work on that project?

22 A. Yes, sir.

23 Q. So, Mr. Munger, when did you first suspect
24 that Microsoft was using your invention?

25 A. Well, as part of that -- that study that --

1 that Mr. Larsen asked us to do, he was very interested
2 in securing instant messages -- instant message and
3 voiceover IP.

4 So we decided to take a look at a live
5 communication server, and one of the engineers that --
6 when we licensed it and installed it, asked me to come
7 into the lab and take a look at a screen.

8 And the screen had a box on the screen, and it
9 had a place to enter a domain name, and underneath there
10 was a button which said the TLS, which stands for
11 Transport Layer Security.

12 And because there was only one button and a
13 domain name, it made me suspicious that it looked very
14 automatic and it -- and it was using a domain name.

15 Q. Did you see anything else that made you
16 suspicious around that time?

17 A. Well, because of that, I went to the internet
18 and saw in the -- in the public literature on the
19 internet the discussion of mutual TLS VPNs between
20 servers.

21 And I also saw literature on peer-to-peer
22 (sic) -- I may not be saying that right -- PNRP, that
23 discussed a domain name and the ability for automatic
24 connections using that domain name.

25 Q. Now, based on what you were able to see with

1 the live communication server screen and the things that
2 you found on the internet, did you know for sure that
3 Microsoft was infringing your patents?

4 A. No, sir.

5 Q. What would you need to see to know for sure?

6 A. You would really have to take a look at the
7 code, the software code that Microsoft is using.

8 Q. Is the Microsoft code available for you to
9 look at?

10 A. No, sir.

11 Q. Can you go out and buy a copy of it?

12 A. No, sir.

13 Q. Can you find it on the internet?

14 A. No, sir.

15 Q. Had you ever seen it?

16 A. No, sir.

17 Q. But is it your understanding that VirnetX has
18 retained an expert, Professor Mark Jones, who has been
19 allowed to see and study the Microsoft source code?

20 A. Yes, sir.

21 Q. And you understand that he will testify about
22 the results of his study later in the trial?

23 A. Yes, sir.

24 Q. Now, what did you do about your suspicions?

25 A. Well, I told -- I told the attorneys at -- at

1 SAIC that had been supporting the team. I told my
2 management superiors. I told the commercialization
3 group that had -- had worked the relationship with
4 VirnetX. And because I was under contract to VirnetX, I
5 told Mr. Kendall Larsen.

6 Q. What did SAIC do after you told them your
7 suspicions that Microsoft was infringing the patents?

8 A. Well, I think they had a couple of independent
9 teams take a look at it, and then they wrote a -- a --
10 there was a letter written to Microsoft.

11 Q. Let me show you Plaintiff's Exhibit 120.

12 MR. POWERS: Your Honor, before we go
13 into this, I'd just like some foundation as to whether
14 this witness was actually aware of this time and
15 involved.

16 We have no objection to the exhibit, as I
17 had previously advised the Court, but right now, there's
18 no foundation that this witness was involved in the
19 letters in any way at the time.

20 THE COURT: All right. Proceed.

21 Q. (By Mr. Cawley) Were you familiar with the
22 effort to try and resolve your suspicions of Microsoft?

23 A. Yes, sir.

24 Q. And were you aware that SAIC was going to
25 communicate with Microsoft?

1 A. Yes, sir.

2 Q. Send them a letter?

3 A. Yes, sir. I -- and I -- I saw this letter at
4 the time that it was sent.

5 Q. Okay. Let's take a look at Plaintiff's
6 Exhibit 120.

7 MR. CAWLEY: First, go, if you would,
8 please, back to the beginning of the letter.

9 Q. (By Mr. Cawley) To whom was the letter
10 addressed?

11 A. It was to Mr. Anoop Gupta.

12 Q. And who was he?

13 A. He was a businessman at Microsoft in the
14 Unified Communications Group.

15 Q. And why was the letter sent to Mr. Gupta?

16 A. Our desire was to have business discussions --

17 Q. Right.

18 A. -- with Microsoft.

19 Q. Okay.

20 MR. CAWLEY: So let's go down now to the
21 body of the letter.

22 Q. (By Mr. Cawley) You see that at the beginning,
23 SAIC indicates to Mr. Gupta that they are writing to
24 introduce an opportunity for SAIC and Microsoft to enter
25 into a mutually beneficial business arrangement in the

1 pursuit of a premiere service offering in the internet
2 communications market.

3 Do you see that?

4 A. Yes, sir.

5 Q. And did this letter to Mr. Gupta identify your
6 patent?

7 A. Yes, sir.

8 Q. And, apparently, just below that, it indicates
9 that a copy of the patent was even sent; is that right?

10 A. Yes, sir.

11 Q. And down below we see that it was requested
12 that SAIC would like to contact Mr. Gupta in the next
13 week or so to discuss the possibility of offering
14 Microsoft a license to the '135 patent; is that right?

15 A. Yes, sir.

16 Q. And you also see that the letter specifically
17 named Live Communications Server 2005 and Microsoft
18 Office Communicator 2005, correct?

19 A. Yes, sir.

20 Q. Now, did Mr. Gupta ever respond to this
21 letter?

22 A. No, sir.

23 Q. Did Microsoft respond to this letter?

24 A. Yes, sir.

25 Q. Let me show you Plaintiff's Exhibit 121.

1 Is this a letter that SAIC received back from
2 Microsoft?

3 A. Yes, sir.

4 MR. CAWLEY: Let's go down to the bottom.

5 Q. (By Mr. Cawley) It's not Mr. Gupta who wrote
6 her, is it? Who wrote her back?

7 A. Their patent counsel.

8 Q. Mr. Jerry -- looks like Gnuschke, Microsoft's
9 Division patent counsel; is that right?

10 A. Yes, sir.

11 Q. And let's take a look at the highlighted
12 portion of this letter.

13 Did he indicate at the conclusion of his
14 letter: I expect, however, that at some point, we will
15 discuss Microsoft patents, which SAIC must license.

16 A. Yes, sir.

17 Q. Did you read this letter when it came in?

18 A. Yes, sir, I did.

19 Q. What was your reaction?

20 A. I found the letter threatening.

21 Q. Did SAIC send another letter?

22 A. Yes, sir.

23 Q. This time to Mr. Gnuschke?

24 A. Yes, sir.

25 Q. Let me show you Plaintiff's Exhibit 98.

1 Is this a letter that was sent back to
2 Mr. Gnuschke in June of 2006?

3 A. Yes, sir.

4 Q. And in addition to this letter back to
5 Mr. Gnuschke, did SAIC attempt to call Mr. Gupta, the
6 Microsoft businessman that they had sent the first
7 letter to?

8 A. Yes, sir.

9 MR. POWERS: Object, no foundation,
10 unless this witness was involved, Your Honor. The
11 foundation hasn't been laid.

12 THE COURT: Lay the foundation.

13 Q. (By Mr. Cawley) Were you involved in
14 discussions about how to contact Mr. Gupta?

15 A. I received this information from Kendall
16 Larsen, who was having weekly meetings with Ms. Boone,
17 and she -- in those weekly meetings, she was telling him
18 that she was trying to make that contact, and he told
19 me.

20 So that's the foundation of my knowledge, sir.

21 MR. POWERS: In that case, Your Honor,
22 I'm going to object to double hearsay and move to
23 strike.

24 THE COURT: All right. Sustained.

25 Q. (By Mr. Cawley) What did you decide around

1 this time, Mr. Munger, had to be done to make your
2 invention a success?

3 A. We felt that we were going to have to defend
4 our patents so that we had an opportunity to go into the
5 market and compete.

6 Q. And what were you going to do in order to make
7 that happen?

8 A. I made the decision with the counsel and with
9 the advice and discussions with managers and both
10 VirnetX and SAIC to move over to VirnetX.

11 Q. So did you leave SAIC and join VirnetX?

12 A. Yes, sir, I did.

13 Q. Why did you do that?

14 A. I thought that they were going to need more
15 inventors to help them, technically. They did not have
16 a lead technical manager. And also that -- to support
17 whatever was needed to protect our patents, sir.

18 Q. What is your position at VirnetX?

19 A. I'm the chief technology officer, and I'm an
20 employee, a member of the Board of Directors.

21 Q. Do you own stock in the company?

22 A. Yes, sir.

23 Q. How much of the company do you own?

24 A. Approximately 2-1/2 percent.

25 Q. Around this time, did SAIC decide that it

1 would re-do its deal or arrangement with VirnetX?

2 A. Yes, sir.

3 Q. What were the terms of the new arrangement?

4 A. The new arrangement was that VirnetX would
5 take the lead in the litigation, and when I came over,
6 the idea at SAIC was that we would still be taking that
7 lead. VirnetX would take the lead.

8 And there was -- the patents would be
9 transferred over to VirnetX, and there was a
10 rearrangement in the splits of -- of revenue.

11 Q. And what was that?

12 A. Is that as a result of settlement or -- or
13 litigation, that VirnetX would get 65 percent, and SAIC
14 would get 35 percent.

15 Q. And in fact, were the patents transferred,
16 pursuant to this new arrangement, from SAIC to VirnetX?

17 A. Yes, sir, they were.

18 Q. And I'll show you Plaintiff's Exhibit 10?

19 Is this a copy of a filing with the Patent
20 Office that contains copies of the assignments of the
21 patents from SAIC to VirnetX?

22 A. Yes, sir.

23 Q. Now, did you -- have you learned that
24 Microsoft eventually responded to that second letter
25 from SAIC?

1 A. I did, sir.

2 Q. Let me show you Defendant's Exhibit 3015.

3 Is that the letter from Microsoft?

4 A. (No response.)

5 Q. And what's the date of that letter?

6 A. September 12th, 2006.

7 Q. So SAIC's second letter was written in June
8 2006?

9 A. Yes, sir.

10 Q. And this letter responding did not -- was not
11 dated until September of 2006, right?

12 A. That's correct, sir.

13 Q. Three months later?

14 A. Yes, sir.

15 Q. By this time, were you gone from SAIC?

16 A. Yes, sir. I was gone in July.

17 Q. Did you ever see this letter before this
18 lawsuit started?

19 A. No, sir.

20 Q. As far as you know, did anyone at VirnetX even
21 know about this letter from Microsoft?

22 A. No, sir.

23 Q. How has -- how has VirnetX gone about
24 defending its patent rights?

25 A. It -- it raised money and filed suit for this

1 trial, sir.

2 Q. And what became of the rest of the team, your
3 team of inventors?

4 A. On the following spring, Dr. Bob Short came
5 over, and by the summer, we had two more of the
6 coinventors and a software developer that had been
7 working with us on the project.

8 Q. So all four of the inventors of one patent now
9 work at VirnetX; is that right?

10 A. That's correct, sir.

11 Q. And on the other patent, four of the five
12 inventors work there?

13 A. Yes, sir.

14 Q. What about the one who doesn't?

15 A. He left SAIC around the year 2000, sir.

16 Q. Now, have you, at VirnetX, continued to work
17 to develop software that uses your invention?

18 A. Yes, sir.

19 Q. Why have you done that?

20 A. There's three reasons.

21 The first reason is that -- and it's called
22 Gabriel. We'll probably hear a lot about that during
23 the trial here.

24 Q. Is that the name you've given the VirnetX
25 software that uses your invention, Gabriel?

1 A. That's right, sir.

2 Q. Okay. Why have you chosen to continue to
3 develop the Gabriel software?

4 A. Gabriel software provides a basis for offering
5 a secure domain name service so that people can get
6 domain names and instantly connect by VPNs.

7 We are talking to companies that may want to
8 license the technology, and the source code is
9 foundation code to allow them to put the capability into
10 their products, if that's worthwhile for them, and also
11 to support this trial.

12 Q. What do you mean to support this trial?

13 A. Well, we didn't know that we would -- you
14 know, we had already started the -- the litigation, that
15 we wanted to be able to demonstrate our invention in
16 court.

17 Q. Is the Gabriel software finished?

18 A. No, sir.

19 Q. What stage is it in?

20 A. It's now in a beta stage, and we have gone out
21 and are having a few people give us advice and -- and --
22 and test it, sir.

23 Q. Now, does software like Gabriel have to work
24 on a computer with an operating system?

25 A. Yes, sir.

1 Q. What operating system did you choose to design
2 Gabriel to work with?

3 A. Microsoft Windows.

4 Q. Why did you make that choice?

5 A. Ninety percent of the computers in the world
6 are running Windows operating systems, so it was -- it
7 was an obvious choice to want to make sure our product
8 was going to run on the majority of the computers.

9 Q. And does Gabriel also use something called
10 Microsoft crypto libraries?

11 A. Yes, sir.

12 Q. What are they?

13 A. Well, crypto libraries are software modules
14 that if I put in plain English, like Hi, Mom, it will
15 scramble it, and then bring it back, and you can
16 transmit the scrambled part.

17 And on the other side, if you use that module
18 on the other side, it will unscramble it, and the Hi,
19 Mom will come out.

20 Q. And are these crypto libraries made available
21 for the use of software developers who write
22 applications that work on Microsoft operating systems?

23 A. Yes, sir.

24 Q. Why did you use them for Gabriel?

25 A. Well, Microsoft has very good libraries,

1 crypto libraries, and there was no reason for us to
2 develop our own, so we're using what's available in the
3 Windows operating system, sir.

4 Q. Have you had any interest in Gabriel?

5 A. Yes, sir.

6 Q. Let me show you Plaintiff's Exhibit 977.

7 What is this document?

8 A. This is a letter of intent between VeriSign,
9 Incorporated, and VirnetX.

10 Q. And what is the letter of intent for?

11 A. We're doing a 90-day study, both technical and
12 business-wise, to look at the opportunity of providing
13 secure domain name services for -- for handheld devices.

14 Q. Smartphones, for example?

15 A. Yes, sir.

16 Q. Who is VeriSign?

17 A. Well, VeriSign is the company that runs the
18 present domain name service for a dot com, like an
19 amazon.com and dot net and dot org. So they've got a
20 lot of experience in providing that kind of service, and
21 they have an infrastructure that's scaled to do that
22 worldwide.

23 Q. And when did VirnetX enter into this letter of
24 intent with VeriSign?

25 A. In December, sir.

1 Q. December of what year?

2 A. 2009.

3 Q. 2009.

4 A. Yes, sir.

5 Q. Now, Mr. Munger, do you think that you and
6 your company can ever be successful in selling your
7 invention for internet security while Microsoft is still
8 infringing?

9 A. No.

10 MR. POWERS: Objection, Your Honor.
11 There's no foundation that Microsoft is infringing.

12 THE COURT: Overruled.

13 Q. (By Mr. Cawley) I'm sorry. What was your
14 answer?

15 A. No, sir.

16 Q. Why do you say that?

17 A. I say that, because if they are infringing,
18 they have the resources to -- to make it very difficult
19 for us to compete.

20 Q. Thank you, Mr. Munger.

21 MR. CAWLEY: I'll pass the witness, Your
22 Honor.

23 THE COURT: All right. Ladies and
24 Gentlemen of the Jury, it's 10 minutes till 3:00. I
25 think we'll take our afternoon break at this time.

1 We'll be in recess until 4:10 (sic).

2 COURT SECURITY OFFICER: All rise for the
3 jury.

4 (Jury out.)

5 (Recess.)

6 (Jury out.)

7 COURT SECURITY OFFICER: All rise.

8 THE COURT: Please be seated.

9 I understand there's an issue before we
10 bring the jury in?

11 MR. POWERS: Yes, Your Honor, there is,
12 and it came up just in the last direct examination.

13 Mr. Munger referred to two potential
14 demonstrations that Mr. Short was going to give, and one
15 of those we had had notice of and had a chance to do an
16 inspection pursuant to the pretrial order, but one of
17 them we had not. And let me just describe briefly what
18 they are so the issue is framed.

19 We were told, pursuant to the pretrial
20 order, on time, with no objections, they were going to
21 do a demonstration of the Gabriel software that we've
22 heard about. And we went over and did that inspection.

23 We were not told that they were going to
24 do a demonstration of the complexity or the attempt to
25 set up some sort of prior art VPN, and that was just

1 alluded to by Mr. Munger in his testimony about what
2 Mr. Short is intending to do.

3 And so if there is an intent to do that
4 demonstration, then we would object, because we did not
5 receive notice of it pursuant to the order, had no
6 opportunity to inspect it, and we would object, although
7 they did follow exactly the right procedure as to
8 Gabriel, and we have no objection to that.

9 THE COURT: All right.

10 MR. CAWLEY: That was a misstatement by
11 the witness or maybe me, Your Honor. He's not going to
12 demonstrate a piece of software. He's going to talk
13 about an exhibit that is in evidence.

14 THE COURT: All right.

15 MR. POWERS: In that case, we don't have
16 a problem.

17 THE COURT: Okay. And why don't y'all
18 just talk during the break about that. I think that
19 could have been resolved.

20 MR. POWERS: I would have, but the
21 statement was so clear on the record that it seemed a
22 clear statement of intent, so I thought we should raise
23 it.

24 THE COURT: All right. Bring the jury
25 in, please.

1 COURT SECURITY OFFICER: All rise for the
2 jury.

3 (Jury in.)

4 THE COURT: All right. Please be seated.
5 All right, Mr. Powers. You may proceed.

6 MR. POWERS: Thank you, Your Honor.

7 May I approach with some exhibits that
8 may be entered?

9 THE COURT: Yes, you may.

10 CROSS-EXAMINATION

11 BY MR. POWERS:

12 Q. Good afternoon, Mr. Munger.

13 A. Good afternoon, sir.

14 Q. I'd like to begin at the part of your
15 testimony where you were describing the work you did
16 with In-Q-Tel to get started on the projects that led to
17 the inventions you patented.

18 A. Yes, sir.

19 Q. Now, I believe you testified that In-Q-Tel is
20 what -- is the entity that gave you the initial funding
21 to do the work that led to the patents-in-suit; is that
22 true?

23 A. That's true, sir.

24 Q. And In-Q-Tel did that work -- gave you that
25 money, and that was about \$3.5 million?

1 A. Yes, sir.

2 Q. They gave that you money before you had
3 actually made the inventions, right?

4 A. That's correct, sir.

5 Q. All right. Now, you then gave the results of
6 your work to In-Q-Tel for their evaluation, didn't you?

7 A. Yes, sir.

8 Q. And you had discussions with In-Q-Tel about
9 what they were -- when they had questions when they were
10 trying to make it work or some question about it, you
11 had some interaction with them during that process,
12 didn't you?

13 A. Yes, sir.

14 Q. So you knew they were using the software you
15 delivered.

16 A. Yes, sir.

17 Q. All right. Now, they then gave it back to
18 you, didn't they?

19 A. I'm not clear on that, sir.

20 Q. All right. In that case --

21 MR. POWERS: Your Honor, may I approach
22 and hand the witness his deposition?

23 THE COURT: Yes, you may.

24 MR. POWERS: Would Your Honor like a
25 copy?

1 THE COURT: No. That's fine.

2 Q. (By Mr. Powers) Mr. Munger, do you recall
3 having your deposition taken in this case?

4 A. Yes, sir.

5 Q. And a deposition is taken under oath, just
6 like the testimony we're having here in Court.

7 A. Yes, sir.

8 Q. Okay. And you recall that we talked about
9 this exact issue in your deposition, about your work
10 with In-Q-Tel, giving them your work, and whether you
11 got it back.

12 A. Yes, sir.

13 Q. And you recall you testified that you did get
14 your work -- your box back from In-Q-Tel?

15 A. That's correct. I did testify at that time
16 that we got it back, sir.

17 Q. All right. And you have no reason to doubt
18 the accuracy of the testimony you gave under oath in
19 your deposition, do you?

20 A. I later learned from Dr. Short, who actually
21 did the thing, that he wasn't sure that it came back to
22 us. But that's the only reason that I have some doubt
23 at this point, sir.

24 Q. But your best testimony that was based on your
25 knowledge was it was returned.

1 A. I thought it was returned when --

2 Q. All right.

3 A. -- I made that statement, sir.

4 Q. And In-Q-Tel, by virtue of funding the work
5 that you did, got a license to the patents and any
6 patents that would come out of it, right?

7 A. Yes, sir, they did.

8 Q. For free, right?

9 A. Yes, sir.

10 Q. And you and SAIC went back to In-Q-Tel to ask
11 for further funding, didn't you?

12 A. Yes, sir.

13 Q. And In-Q-Tel said no, right?

14 A. That's correct, sir.

15 Q. And they said no after they had evaluated the
16 technology you gave them and then returned it, right?

17 A. Yes, sir.

18 Q. Okay. Now, based on your discussions with
19 In-Q-Tel, do you recall that they were unhappy with the
20 performance of the technology that you had given them?

21 A. No, sir.

22 Q. Well, let's see if we can refresh your
23 recollection.

24 Do you -- let me first ask you a simple
25 question. Do you know, at In-Q-Tel, someone named Don

1 Brezinski?

2 A. Yes, sir. That name is familiar to me.

3 Q. That's one of the people that you were dealing
4 with there?

5 A. Yes, sir, I believe so.

6 Q. And do you know someone at In-Q-Tel named Joy
7 Dorman, a woman named Joy Dorman?

8 A. That one doesn't ring a bell.

9 Q. Do you know an Andy Halliday, H-A-L-L-I-D-A-Y?

10 A. That name is -- that name is familiar to me,
11 sir.

12 Q. Also, one of the people you were dealing with
13 there?

14 A. It's likely.

15 Q. And do you know a Gilman Louie, L-O-U-I-E?

16 A. Yes, sir, definitely.

17 Q. Gilman Louie is the President and CEO of
18 In-Q-Tel, right, or was at the time?

19 A. Was at the time, yes, sir.

20 Q. Now, do you recall that In-Q-Tel's decision
21 not to re-fund your research was made in the 2001 time
22 period?

23 A. Yes, sir.

24 Q. Did you ever hear or learn from anyone that
25 Mr. Louie, the CEO of In-Q-Tel, said the NetEraser

1 project should be placed in the living dead category or
2 any words to that effect?

3 A. Not until today, sir.

4 Q. Did you -- do you recall hearing that
5 Mr. Brezinski, which is B-R-E-Z-I-N-S-K-I, felt the
6 project that you had led did not live up to the
7 expectations? Ever hear anything to that effect?

8 A. No, sir.

9 Q. I'd like you to look at Exhibit 31 and 32, DX
10 31 and 32. It's in the binder I just put in front of
11 you.

12 You learned of the decision by In-Q-Tel not to
13 fund the continuation of your research. You did learn
14 that, didn't you?

15 A. Yes, sir.

16 Q. And that was about the June -- June 2001 time
17 period?

18 A. Yes, sir.

19 Q. And is it your testimony that you had no idea
20 what the reason for that decision was?

21 A. Yes, sir. I had an understanding of why they
22 weren't going to fund it.

23 Q. If you turn to Page 3 of Exhibit 3132.

24 MR. POWERS: And, Chris, could you blow
25 up the bottom paragraph, please.

1 Q. (By Mr. Powers) Let me know when you have that
2 in front of you, Mr. Munger. Do you see that?

3 The first sentence says Mr. Brezinski and
4 Ms. Dorman commented that the product had not lived up
5 to expectations. This is under the heading of
6 Mr. Halliday giving an overview of the NetEraser
7 project.

8 Do you see that?

9 A. Yes, sir.

10 Q. Did that help refresh your recollection that
11 one of the reasons that In-Q-Tel did not fund the
12 completion of your work was that the technology you had
13 given them did not live up to expectations?

14 A. No, sir.

15 Q. You just don't -- you just don't recall one
16 way or the other?

17 A. Well, I don't -- I never got that kind of
18 negative feedback in my discussions with them, sir.

19 Q. If you turn to the next page --

20 MR. POWERS: Chris, could you bring that
21 sentence from Mr. Louie?

22 Q. (By Mr. Powers) It says: Mr. Louie commented
23 that the NetEraser project should be placed in the,
24 quote, living dead category, close quote, with little or
25 no attention paid to it.

1 Does that help you recall that you heard
2 something to that effect during the same time period
3 when In-Q-Tel decided not to fund?

4 A. No, sir.

5 Q. It is true, though, that just about that time,
6 In-Q-Tel decided -- did decide not to fund your project,
7 right?

8 A. That's a correct statement, sir.

9 Q. All right. That's correct or incorrect?

10 A. That's correct.

11 Q. Okay. Thank you.

12 So you know, don't you, that In-Q-Tel and the
13 CIA don't actually use the technology that you gave
14 them.

15 A. I can't say that for sure, sir.

16 Q. That's what you believe, isn't it?

17 A. I -- I really couldn't say, sir.

18 Q. Well, let's look at your deposition, and look
19 at the April 23 deposition at Page 87. Let me know when
20 you have it.

21 And I'll read it from Page 87 in your April
22 23rd deposition, Lines 21 through 24.

23 QUESTION: Do you know whether any government
24 entity is using the technology developed by SAIC?

25 ANSWER: I do not know of any government

1 entity using the technology developed by SAIC.

2 That was what your testimony at deposition,
3 wasn't it, Mr. Munger?

4 A. Yes, sir. That's a correct statement.

5 Q. And it was true then?

6 A. Yes, sir.

7 Q. And true now?

8 A. Yes, sir.

9 Q. All right. Now, let's talk about your
10 company, your employer at the time, SAIC, and its
11 support of your -- of your project.

12 Now, you -- you referred in your direct
13 testimony to the CEO of SAIC.

14 Do you recall that?

15 A. Yes, sir.

16 Q. And who's he?

17 A. Dr. Bob Beyster at the time, sir.

18 Q. And you made a presentation to the CEO in
19 March of 2000 seeking funding, didn't you?

20 A. I was one of the presenters, yes, sir.

21 MR. POWERS: Could you bring up DX3139,
22 please, Chris?

23 Q. (By Mr. Powers) And let me know when you have
24 it in front of you, Mr. Munger.

25 A. What was the number again, sir?

1 Q. 3139.

2 Do you have it in front of you?

3 A. Yes, sir, I do.

4 Q. Great. Thank you.

5 This is the presentation you were just
6 referring to?

7 A. That was one of -- one of the presentations,
8 yes, sir.

9 Q. And it's a presentation that you prepared part
10 of and presented part of, correct?

11 A. I did not author most of this presentation,
12 sir.

13 Q. But part of it, you did?

14 A. It's -- it's likely I could have contributed
15 to it, yes, sir.

16 Q. Okay. And it's a presentation that you --
17 that was for, at least in part, requesting funding for
18 your project from Dr. Beyster, correct?

19 A. Yes, sir.

20 Q. All right. And if you turn to Page 5 of the
21 document -- and I'll be referring to the -- there's a
22 lot of pages -- page numbers in these documents. I'll
23 be referring to the one in the bottom right-hand corner
24 where it will say -- it will have the exhibit number and
25 then .005 or .05, just because it'll make it easier.

1 A. Thank you.

2 Q. Do you have that in front of you?

3 A. Yes, sir, I do.

4 Q. Now, if you go to the last bullet --

5 MR. POWERS: Chris, could you bring that
6 up, please?

7 Q. (By Mr. Powers) -- this is the description to
8 your CEO about the current environment addressing your
9 proposed technology, right?

10 A. Yes, sir.

11 Q. And one of the aspects of the -- of the
12 current environment was that there were a lot of
13 companies addressing the same issue you were going
14 after, and you said, quote, the race is on, exclamation
15 mark, close quote, right?

16 A. Yes, sir.

17 Q. So it's true that as of this March of 2000
18 time period, there were a lot of different companies
19 trying to address the same problem that you were
20 thinking about, and you knew you were in a race with
21 those companies, true?

22 A. Yes, sir. This -- this timeframe was not
23 necessarily about present technology. It was a year
24 before Beyster's discussions later.

25 Q. This -- this presentation to him was in March

1 of 2000, right?

2 A. Yes, sir.

3 Q. And the title of this particular page is the
4 current environment, right?

5 A. Yes, sir.

6 Q. So your group was trying to convey to your CEO
7 what the current environment was that you were going to
8 be competing against, right?

9 A. Yes, sir.

10 Q. And you knew that you were in a race against
11 several other companies addressing the same problem; is
12 that fair?

13 A. Yes, sir.

14 Q. Okay. Now, in this document in March of 2000,
15 you asked Dr. Beyster to support and agree to an
16 investment of \$7 million in your project, right?

17 A. I was part of the group that did that, yes,
18 sir.

19 Q. And the number you asked for was \$7 million?

20 A. I don't know. I'd have to refresh my memory.

21 Q. Go to Page 26.

22 A. 26? Thank you.

23 Q. The page that's called Recommendation. Let me
24 know when you're there.

25 A. Yes, sir, I see that.

1 Q. And the recommendation that's included in the
2 box in bold at the bottom is: Commit \$7 million of
3 staged investment now, right?

4 A. Yes, sir.

5 Q. That's what you and your team were requesting
6 the CEO of your company to agree to, true?

7 A. Yes, sir.

8 Q. And Dr. Beyster did not agree to commit that 7
9 million, did he?

10 A. That's correct.

11 Q. In fact, Dr. Beyster and SAIC invested \$7
12 million in Aventail, didn't they?

13 A. Yes, sir, later.

14 Q. Now, let's go forward to June of 2001, which
15 is that same -- June of 2001 was the same time period
16 that In-Q-Tel was saying: We're not going to fund
17 anymore.

18 Do you recall that?

19 A. Yes, sir.

20 Q. It was in that same time period that SAIC
21 said, not only we're not going to give you 7 million
22 more dollars, we're going to, quote, pull the plug,
23 close quote. That's true, isn't it?

24 A. Yes, sir.

25 MR. POWERS: Could you pull up DX3141,

1 please.

2 Q. (By Mr. Powers) Let me know when you have it.

3 A. I have it, sir.

4 Q. Okay. Now --

5 MR. POWERS: First, let's bring up the --
6 Chris, if you could, the to and the from. Bring that up
7 a little larger so we can see it. Maybe it's just me.
8 That's better.

9 Q. (By Mr. Powers) The e-mail is dated June 18 of
10 2001, and it's from a Mr. Edward Hendrick.

11 Do you see that?

12 A. Yes, sir, I do.

13 Q. Edward Hendrick was an SAIC executive,
14 correct?

15 A. Yes, sir.

16 Q. And he was the executive involved in the
17 process of deciding whether to commercialize and support
18 the research project you were working on, true?

19 A. Yes, sir.

20 Q. In the first paragraph --

21 MR. POWERS: And, Chris, if you could
22 bring that up, please.

23 Q. (By Mr. Powers) -- it says: Thought you would
24 like to know that Duane and Don Foley made the decision
25 last week to pull the plug on VirnetX and return to

1 trying to get additional government funding to continue
2 development of the technology.

3 Do you see that?

4 A. Yes, I do, sir.

5 Q. You were told in this June of 2001 time
6 period, that your company had decided to pull the plug
7 on your project?

8 A. Yes, sir.

9 Q. And you knew that the reason for that was the
10 success of one of your competitors, Aventail; is that
11 right?

12 A. That's one of the reasons, yes.

13 MR. POWERS: Chris, if you could pull
14 up -- pull up the last paragraph, please. Sorry, the
15 next to the last paragaraph.

16 And that's just not going to be legible
17 at least to my old eyes, but let's see if I can read it.

18 Can you make that any larger?

19 And Chris has that look on his face that
20 means no, so I'll just read it.

21 Q. (By Mr. Powers) It says: From my perspective,
22 the straw that broke the camel's back was the loss of
23 the ANX beta site as they decided to go with an Aventail
24 solution.

25 Now, let's -- let's stop there for a

1 minute and make sure we know who we're talking about.

2 It says ANX beta site. ANX was a company that SAIC
3 owned, true?

4 A. That's true, sir.

5 Q. And one of the things that had happened during
6 the discussions with Dr. Beyster and internally within
7 SAIC was the need to get somebody to prove the
8 technology at a beta site, true?

9 A. True, sir.

10 Q. And you tried to get a lot of people to serve
11 as that beta site to take your technology and prove that
12 it could work. That's what you were trying to do at the
13 time, right?

14 A. Yes, sir.

15 Q. And, in fact, Dr. Beyster, your CEO,
16 specifically said: I'd like that beta site to be ANX,
17 which SAIC owned, true?

18 A. I'm sorry. Would you repeat that question?

19 Q. Sure. In addition to you generally wanting
20 beta sites to prove the technology, your CEO,
21 Dr. Beyster, said he wanted you to use ANX as a beta
22 site.

23 A. Yes, sir, that's correct.

24 Q. And instead of choosing your technology for
25 the beta site, ANX chose Aventail's, right?

1 A. That's correct, sir.

2 Q. And Aventail was a competing technology
3 offering a secure, easy form of internet access, true?

4 A. Yes, sir, I assume so.

5 Q. Now, the next sentence after the part I read
6 says, quote, incidentally, SAIC is considering an
7 investment in Aventail.

8 You knew that at the time, around June of
9 2001?

10 A. I didn't know that until it came up as part of
11 the preparation for the trial, sir.

12 Q. But you did learn that SAIC, in fact, invested
13 \$7 million in Aventail in late 2001.

14 A. That's a correct statement, sir.

15 Q. And, in fact, that investment in Aventail of
16 \$7 million came after 9/11, didn't it?

17 A. Yes, sir.

18 Q. So let's talk for just a minute about your
19 attempts to get various types of entities, various types
20 of companies, interested in your technology. You
21 testified about some of this on your direct examination,
22 correct?

23 A. Yes, sir.

24 Q. Now, one of the groups that you testified
25 about was a venture capitalist. You testified you met

1 with about 30 and that none of them agreed to fund your
2 technology.

3 Do you recall that?

4 A. Yes, sir, I do.

5 Q. But did you actually have meetings with them,
6 didn't you?

7 A. Probably not all 30, but it was a large
8 number, yes, sir.

9 Q. And you personally helped attend those
10 meetings to give a demonstration of and an explanation
11 of the technology that you thought they should be
12 interested in, true?

13 A. An explanation, yes, sir.

14 Q. And after receiving -- and they, at least
15 those that met with you, were interested enough to meet,
16 right?

17 A. Yes, sir.

18 Q. And on direct examination, you said, well, it
19 was a horrible time, because there was a recession, and
20 people didn't want to do this type of investment. They
21 were at least interested enough to meet with you and
22 hear what you had to say and hear your explanation of
23 your technology, true?

24 A. Yes, sir.

25 Q. But after hearing it, they said no; is that

1 correct?

2 A. That's correct, sir.

3 Q. Now, another avenue, another path that you
4 went down was to try to get companies who would be
5 involved in internet-type transactions interested in
6 potentially using or partnering with your technology,
7 true?

8 A. Yes, sir.

9 Q. And you described a few of them. I believe
10 you said Morgan Stanley, eBay, and Amazon, right?

11 A. Yes, sir.

12 Q. And there were more than that, weren't there?

13 A. There could be. I just don't recall the
14 others as much.

15 Q. There were a large number, weren't there?

16 A. I don't know how -- what a large -- you know,
17 it could have been twice that number, yes, sir.

18 Q. Now, when you -- and when you personally went
19 to those companies, you gave an explanation of the
20 technology and how it worked and what it could
21 accomplish and tried to sell it to them, right?

22 A. Yes, sir.

23 Q. And each of them said, thank you, but no thank
24 you; is that fair?

25 A. That's correct, sir.

1 Q. Now, let's talk about SafeNet for a minute.
2 You -- you testified in your direct examination that
3 SafeNet was interested in your technology in the summer
4 of 2002, true?

5 A. Yes, sir.

6 Q. And that they entered into a license agreement
7 and then later terminated it, right?

8 A. Yes, sir.

9 Q. Now, you also -- and you said that it
10 terminated because customers weren't interested, and
11 there really wasn't a market for it.

12 Do you recall that testimony?

13 A. Yes, sir.

14 Q. But SafeNet also received your information
15 about your technology, true?

16 A. That's correct, sir.

17 Q. And you're aware that SafeNet did a technical
18 evaluation of your technology?

19 A. I -- I assume that they did, yes, sir.

20 Q. You knew Mr. Becker at SafeNet?

21 A. Yes, sir.

22 Q. And you know that he was a technical person
23 there who was evaluating your technology from a
24 technical point of view?

25 A. Yes, sir.

1 Q. And did you learn from Mr. Becker that he was
2 unsatisfied with your technology?

3 A. No, sir.

4 Q. Did Mr. Becker ever tell you personally or did
5 you hear from any source that Mr. Becker thought your
6 technology did not make connecting easier?

7 A. No, sir, I don't recall that.

8 Q. Now, you testified that SafeNet terminated the
9 agreement, and you showed us the letter which did so.

10 Do you remember that on direct examination?

11 A. Yes, sir.

12 Q. And SafeNet did so at the time when it had a
13 right to terminate without paying SAIC any money, true?

14 A. That's correct, sir.

15 Q. So despite the 20 percent that you testified
16 about, SafeNet actually paid nothing; isn't that right?

17 A. That's correct, sir.

18 Q. And they did that after they evaluated your
19 technology, true?

20 A. Yes, sir.

21 Q. Now, you also testified, I believe, that you
22 met a man by the name of Kendall Larsen. Let's talk
23 about him a bit.

24 Did you first meet him in connection with a
25 SafeNet discussion or a SafeNet-related discussion?

1 A. Yes, sir, I did.

2 Q. And at that time, Kendall Larsen -- and I'll
3 say Kendall Larsen to distinguish him from other Larsons
4 that are in this case -- Kendall Larsen was at a company
5 called Phoenix, true?

6 A. That's correct, sir.

7 Q. And you went to Phoenix to make a presentation
8 to try to get them interested in your technology, true?

9 A. Yes, sir.

10 Q. And they said thank you, but no thank you?

11 A. That's correct, sir.

12 Q. And immediately thereafter, Mr. Larsen left
13 Phoenix and went to a company called Osprey Ventures,
14 true?

15 A. Yes, sir.

16 Q. And asked you to come in and make a
17 presentation to Osprey to try to get them interested in
18 funding your proposal, right?

19 A. Yes, sir.

20 Q. And they said thank you, but no thank you; is
21 that fair?

22 A. That's fair, sir.

23 Q. All right. So in this summer of 2001 time
24 period when In-Q-Tel had decided not to fund --

25 A. (Sneezes.) Excuse me.

1 Q. Bless you.

2 When In-Q-Tel had decided not to fund your
3 project and SAIC had decided to pull the plug, at that
4 point, SAIC tried to work its government connections to
5 get funding, true?

6 A. Yes, sir.

7 MR. POWERS: And, Chris, if you could put
8 up from the opening Page 11.

9 Q. (By Mr. Powers) Is this a fair summary of the
10 government entities to which you tried to get interest
11 in your technology?

12 A. I can certainly verify all, and I don't
13 remember the FAA, but it's -- that's a possibility,
14 also.

15 Q. So at least in terms of what's on Page 11, you
16 recall trying to get the CIA, Homeland Security, the
17 FBI, OSIS, and DARPA all interested in your technology
18 and -- is that true?

19 A. That's correct, sir.

20 Q. And they all said no?

21 A. That's correct, sir.

22 Q. And they said no despite the fact that SAIC
23 has very good connections with those agencies, true?

24 A. Yes, sir.

25 Q. It works with those agencies on a regular

1 basis, and that's its primarily business, is the federal
2 government, right?

3 A. Yes, sir.

4 Q. And they said no despite the fact that the
5 government has a free license to your patents, true?

6 A. Yes, sir.

7 Q. Now, the FAA -- let's just look at that
8 briefly.

9 MR. POWERS: Could you bring up 3525,
10 please. DX3525. I think that's the wrong exhibit.

11 Could you bring up DX3268. 3268.

12 Let's bring up the first page, please,
13 Chris, and blow that part up.

14 Q. (By Mr. Powers) Mr. Munger, is Exhibit 3268 is
15 a typical type of presentation you were making to these
16 government agencies?

17 A. Yes, sir, it is.

18 Q. You used pretty much the same presentation for
19 each one of them?

20 A. With variation, yes, sir.

21 Q. Okay. And your primary pitch to each of these
22 government agencies, the argument you made to try to
23 sell them, was that you could have easy, fast, secure
24 internet access for their use, true?

25 A. Yes, sir. That was one of the key aspects

1 that we presented.

2 Q. And they all said no?

3 A. Yes, sir, they said no.

4 Q. Now, with respect to Kendall Larsen for a
5 moment, after he moved from Phoenix to Osprey, he then
6 moved from Osprey to being on his own, right?

7 A. Yes, sir.

8 Q. And that was the point at which he was trying
9 to raise money to start what became the company VirnetX,
10 not the technology VirnetX; is that fair?

11 A. Yes, sir.

12 Q. All right. Now -- and Mr. Larsen became the
13 CEO of VirnetX once it was formed?

14 A. Yes, sir.

15 Q. And there was a period of six months to a year
16 when VirnetX was formed as a company and Mr. Larsen was
17 running it where you weren't at VirnetX; you were still
18 at SAIC, true?

19 A. That's true, sir.

20 Q. Okay. Let's talk about -- well, one other
21 prior art technology that you described in your direct
22 examination was https.

23 Do you recall that?

24 A. Yes, sir.

25 Q. Now -- and you said that htp -- https is

1 what's typically used when we do a credit card swipe at
2 the grocery store or at Wal-Mart, true?

3 A. I -- I don't know that for sure, but it's
4 possible, yes.

5 Q. That's your understanding, isn't it?

6 A. I -- I don't know how the swipe machine works
7 at Wal-Mart, sir.

8 Q. Well, but you do understand that https is the
9 standard way that commercial financial transactions are
10 protected around the internet. I believe that's what
11 you testified on your direct examination; is that right?

12 A. I -- I know https from a client to a browser
13 to order a book on a server. I don't know other uses in
14 the back end of business.

15 Q. All right.

16 A. But I do understand that, sir.

17 Q. That's fair enough. So let's take that
18 example.

19 So if you were going to amazon.com and
20 ordering a book, you understood that that transaction,
21 when you give the credit card number, et cetera, was
22 treated by https, true?

23 A. True.

24 Q. That https is easy. You don't have to do
25 anything. You just plug in your credit card and say

1 order, right?

2 A. Yes, sir.

3 Q. Very easy, very fast.

4 A. Yes, sir.

5 Q. And secure, right?

6 A. Yes, sir.

7 Q. Now, let's go back in time to 1998. And you
8 testified on your direct examination that you had this
9 idea, and you wrote this paper called Aladdin in August
10 of 1999.

11 Do you remember that testimony?

12 A. Yes, sir, I do.

13 Q. Now, in fact, you had actually gone to a DARPA
14 meeting in February of 1998 on this subject, security on
15 the internet, hadn't you?

16 A. No, sir.

17 Q. You had not? All right. So let's talk about
18 that.

19 MR. POWERS: Let's bring up Exhibit 3418,
20 DX3418.

21 Q. (By Mr. Powers) Let me know when you have it
22 in front of you, Mr. Munger.

23 A. That's 3148?

24 Q. 3418.

25 A. Oh, I'm sorry. I apologize. I have it, sir.

1 Q. This is a DARPA information assurance
2 principal investigators' meeting in February of 1998 in
3 Annapolis, Maryland?

4 A. Yes, sir.

5 Q. And Annapolis is very near your house, isn't
6 it?

7 A. Yes, sir, that's correct.

8 Q. You went to this particular meeting, didn't
9 you?

10 A. No, sir.

11 Q. You were aware of this meeting, though,
12 weren't you?

13 A. No, sir.

14 Q. Do you recall submitting a proposal to DARPA
15 that related to the discussion of this meeting?

16 A. No, sir.

17 Q. Let's look at the proposal.

18 Now, could you look at Exhibit DX3541? Let me
19 know when you have it.

20 A. I have it, sir.

21 MR. POWERS: Chris, let's bring up the
22 very first -- just the part at the top. Perfect.

23 Q. (By Mr. Powers) Now, let's make sure we
24 understand what the terminology means.

25 Information Assurance BAA Outline. Do you see

1 that?

2 A. Yes, sir, I do.

3 Q. You know what that means, don't you?

4 A. Yes, sir.

5 Q. BAA Outline is an organization related to
6 DARPA that you submit proposals to for funding?

7 A. Yes, sir.

8 Q. And Exhibit 3541 is an internal SAIC draft of
9 a response to a request by DARPA for proposals for
10 funding, right?

11 A. Yes, sir.

12 Q. And so this is an internal draft that you had
13 some role in preparing?

14 A. Yes, sir.

15 Q. And so the point of this was to submit
16 something to DARPA that would ask them to get funding
17 for your NetEraser project, fair?

18 A. That's correct, sir.

19 Q. Now, let's talk about DARPA for a minute.
20 DARPA stands for Defense Advanced Research Projects
21 Agency?

22 A. That's correct, sir.

23 Q. So this is an agency designed to fund
24 development of technology that might be useful for the
25 government, particularly, the Department of Defense?

1 A. Yes, sir.

2 Q. And DARPA is very involved in the internet,
3 aren't they?

4 A. Yes, sir.

5 Q. And internet security?

6 A. Yes, sir.

7 Q. Now -- and the proposal that you were seeking
8 funding for was your NetEraser project. You wanted
9 funding from DARPA as part of that, right?

10 A. Yes, sir, the address hopping.

11 Q. Now, when you were preparing this proposal,
12 one of the -- there's an outline that you have to follow
13 that DARPA gives you, and you have to fill -- fill in
14 responses throughout, true?

15 A. That's correct, sir.

16 Q. So if you could turn to Exhibit 3541 to
17 Page 6.

18 MR. POWERS: And, Chris, if you could
19 pull up Section J that starts in italics all the way
20 down to the last bullet underneath it. Let's just look
21 at that.

22 Q. (By Mr. Powers) Let me know when you have it.

23 A. Yes, sir.

24 Q. So just to orient ourselves, J is
25 Demonstration and Immigration Plan, the part in italics,

1 and then it says: Offerors should describe how their
2 results could be integrated with solution other than IA
3 contractors currently developing or are likely to
4 develop -- facilitating systematic approaches to the
5 large capabilities described above.

6 That part in italics is the part in the DARPA
7 form that you have to respond to, fair?

8 A. Yes, sir.

9 Q. All right. And the part underneath that,
10 which are all the little bullet points, those are drafts
11 that you and your group created that would be responsive
12 to that point; is that correct?

13 A. Yes, sir.

14 Q. And the second bullet down says, quote, what
15 about the DVPN effort?

16 Do you see that?

17 A. Yes, sir.

18 Q. Now, that refers to dynamic virtual private
19 networks, doesn't it?

20 A. Yes, sir.

21 Q. So you knew in September of '98 about the
22 dynamic virtual private network, didn't you?

23 A. No, sir.

24 Q. Even though you put it in this form to DARPA?

25 A. That's correct, sir.

1 Q. So you put it in the form, but you didn't know
2 anything about it.

3 A. Very little about it.

4 Q. But you knew it was a competitor that was
5 already on the market in '98.

6 A. No, sir.

7 Q. But you knew enough about it to use its right
8 initials, didn't you?

9 A. Yes, sir. The -- there was a list of programs
10 that we had to say we were willing to work with to do
11 demonstrations, and so we were going to list it, and I
12 wrote a question mark, because I probably didn't
13 understand what it was about when I found on their
14 program list.

15 Q. So that statement, what about the DVPN effort,
16 that was actually your question that you put in?

17 A. Yes, sir, I believe I wrote that.

18 Q. And someone answered that question, didn't
19 they, in a later draft?

20 A. To -- enough to put it -- I can't -- I can't
21 remember our response, but we probably listed programs
22 we were willing to work with, yes, sir.

23 Q. Would you look at DX3038, please.

24 A. 3038?

25 Q. 3038.

1 MR. POWERS: Let's bring up the first
2 whole part of it.

3 Q. (By Mr. Powers) Do you have that in front of
4 you Mr. Munger?

5 A. Yes, sir I do.

6 Q. 3038 is a later internal SAIC draft response
7 to DARPA following up on what we just looked at, which
8 was DX3541, right?

9 A. Yes, sir.

10 Q. And if you go to that same spot -- it's on
11 Page 14 this time.

12 MR. POWERS: Let's bring up Section J
13 again, please, Chris.

14 Q. (By Mr. Powers) Let me know when you're there,
15 Mr. Munger.

16 A. I'm there, sir.

17 Q. So you have the same boilerplate sort of form
18 section of demonstration and integration plans, true?

19 A. Yes, sir.

20 Q. And now we have a later draft, internal,
21 written by SAIC, you and your team, about how to respond
22 to that section, correct?

23 A. Yes, sir.

24 Q. And, again, the second bullet down starts off
25 with what about the DVPN effort, which is the same text

1 that we saw in the prior exhibit, true?

2 A. Yes, sir.

3 Q. But now it's filled in. BBN is doing. We are
4 not willing to give this to them. Leave it unsaid,
5 question mark.

6 Did you write that as well?

7 A. I can't recall, but it's very possible that I
8 wrote that, sir.

9 Q. So you knew that BBN -- a company called BBN
10 was doing DVPN, right?

11 A. Yes. I probably discovered that they were one
12 of the contractors in that other DARPA program.

13 Q. So you knew that something called dynamic
14 virtual private networks was being actually used by a
15 company called BBN, right?

16 A. Yes, sir.

17 Q. And you knew that BBN was a competitor of
18 yours.

19 A. Yes, sir.

20 Q. Now let's turn to Exhibit 3107, please, in
21 front of you. Let me know when you have it, Mr. Munger.

22 A. I have it, sir.

23 Q. Thank you.

24 This is the final submission that you gave to
25 DARPA requesting funding, right?

1 A. Yes, sir, it looks like it.

2 Q. And if we go down to Section J -- this time
3 it's at Page 32 of the final text.

4 Do you have that in front of you?

5 A. Yes, sir, I do.

6 Q. The actual final text of your response in
7 Section J runs about a full page, doesn't it?

8 A. Yes, sir.

9 Q. And you don't mention DVPN, the dynamic
10 virtual private network, or BBN's use of it, do you?

11 A. No, sir.

12 Q. And that was the suggestion that you had made
13 in the last draft, leave it unsaid, right?

14 A. We probably didn't feel it was necessary.

15 Q. It wasn't -- you thought it wasn't necessary
16 even though the whole point of this question is how
17 you're going to work with other technologies that DARPA
18 might use, right?

19 A. Yes, sir.

20 Q. That is the question DARPA's asking you in
21 Section J, how will you work with other technologies
22 we're using, right?

23 A. Yes, sir.

24 Q. And you knew that DARPA was working with DVPN.

25 A. Yes, sir, that's one of their programs.

1 Q. So dynamic virtual private networks, you knew
2 was prior art in 1998, being a program within DARPA.
3 You knew that.

4 A. No, sir, I did not know that it had any prior
5 art.

6 Q. Well, you knew it was before your invention.
7 This is '98. You haven't had that magical train ride
8 yet coming back from New York, right?

9 A. That's correct, sir, but I did not know any of
10 the underlying technology in those programs -- that
11 program.

12 Q. But you knew it was being used by a competitor
13 of yours in the same field for network security. You
14 knew that.

15 A. Knew what was being used, sir?

16 Q. DVPN.

17 A. The program name?

18 Q. Yes.

19 A. Yes. There was a program named DVPN, yes,
20 sir.

21 Q. Okay. So let -- now let's talk about
22 Aventail.

23 You also knew that Aventail, as a product,
24 existed before your patents, true?

25 A. No, I don't know that, but I have heard that

1 Aventail had a product out before ours today, sir, yes,
2 sir.

3 Q. And you don't deny that, do you?

4 A. No, sir, I don't deny that.

5 Q. Now, you concluded that ANX was going to be
6 close to your patent claims if it was using Aventail,
7 didn't you -- didn't you?

8 A. I think I made a statement about 14 months
9 before 2000 -- the summer of 2001 in an e-mail that said
10 that, yes, sir.

11 Q. Let's look at DX3339.

12 A. That was 33 --

13 Q. 3339.

14 A. I'm sorry. I'm hearing 3330 --

15 Q. 3339.

16 A. I've got it now, sir.

17 Q. Okay. Is Exhibit 3339 an e-mail that you
18 wrote in May of 2000?

19 A. Yes, sir. I've got no reason to believe that
20 that isn't an e-mail from me.

21 Q. And you write this to Bob Short, Vic Larson,
22 Doug Schmidt, and Thomas Swartz, right?

23 A. Yes, sir.

24 Q. And the subject line says: It's NetEraser and
25 ANX, true?

1 A. That's true, sir.

2 Q. And this is at a time when you're trying to
3 get ANX to be a beta site for your technology, right?

4 A. No, sir. This is well before then.

5 Q. And yet you say, quote, it sounds like ANX is
6 getting very close to touching on our patent claims in
7 DNS, Gif, right?

8 A. Yes, sir, I said that.

9 Q. Now, you testified earlier that you were aware
10 that SAIC, after denying your request for \$7 million,
11 did invest \$7 million in Aventail in 2001.

12 Do you recall that?

13 A. Yes, sir, I do.

14 Q. Let's fix the date on that.

15 MR. POWERS: It will be DX3174.

16 Actually -- I'm sorry -- it's 3474.

17 A. I thought I was losing it.

18 Q. (By Mr. Powers) No. I can't read my own
19 handwriting sometimes.

20 A. 3470?

21 Q. 3474.

22 A. I don't seem to have it, but we can proceed,
23 if it's important.

24 Q. If you don't have it, I'll give you mine.

25 MR. POWERS: May I approach, Your Honor?

1 THE COURT: Yes, you may.

2 A. Thank you.

3 Q. (By Mr. Powers) Does this help refresh -- does
4 Exhibit 3474 help refresh your recollection about the
5 timing of SAIC's investment of \$7 million in Aventail,
6 that it was October of 2001?

7 A. No, sir. I -- I'm afraid that I -- this is
8 something that I only learned in preparation for this
9 trial, sir.

10 Q. But you did know it was post 9/11, that you
11 know.

12 A. I can look at this date and see that, yes,
13 sir.

14 Q. Now, you had earlier testified that one of the
15 things that made it hard for you to get money was that
16 in 2001, there was a recession.

17 Do you recall that?

18 A. Yes, sir.

19 Q. But that recession didn't prevent SAIC from
20 investing \$7 million in Aventail, did it?

21 A. No, sir.

22 Q. And you also testified that one of the
23 problems you faced was that 9/11 caused a re-focus of
24 your energies within SAIC to different areas, true?

25 A. Yes, sir.

1 Q. But SAIC, post 9/11, still invested \$7 million
2 in network security with Aventail even after 9/11.

3 A. That's correct, sir.

4 Q. All right. Now, another technology that you
5 were aware of was a technology called PPTP, true?

6 A. I know the name, yes, sir.

7 Q. And it's Pointe2Pointe Tunneling Protocol?

8 A. Yes, sir.

9 Q. And you knew that that existed before your
10 work on their NetEraser.

11 A. That's correct, sir.

12 Q. And you knew that that was a way of setting up
13 a VPN automatically. You knew that?

14 A. No, sir, I didn't.

15 Q. You know that now, don't you -- don't you?

16 A. I heard your -- your opening, and you say that
17 they have an automatic approach. That's the first time
18 I've heard that, yes, sir.

19 Q. So in all of your investigations of the prior
20 art and the state of the technology that you testified
21 on direct examination, you didn't look at PPTP and how
22 it worked?

23 A. No, sir, we didn't.

24 Q. Now, another technology that pre-dated your
25 work was one called SSL, right?

1 A. Yes, sir.

2 Q. And that's another way of providing network
3 security before your work on NetEraser; is that true?

4 A. Yes, sir, that's true.

5 Q. Let's talk for a minute about what happened
6 when you left SAIC and moved to VirnetX.

7 That was in the summer of 2006, correct?

8 A. July 2006, yes, sir.

9 Q. All right. And when you did so, Kendall
10 Larsen was the CEO of VirnetX at that time, right?

11 A. Yes, sir.

12 Q. And still is today?

13 A. That's correct, sir.

14 Q. And Kendall Larsen is also Chairman of the
15 Board of VirnetX?

16 A. Yes, sir.

17 Q. So he's your boss.

18 A. Yes, sir.

19 Q. And he had been directing -- Kendall Larsen
20 had been directing the technical efforts of VirnetX
21 before you arrived; is that fair?

22 A. That's -- that's correct, sir.

23 Q. And one of the technical efforts that you
24 became aware of when you joined VirnetX was VirnetX's
25 work with a company called Magenic.

1 Do you recall that?

2 A. Yes, sir.

3 Q. Magenic was another different company that
4 VirnetX had hired to do some technical work on your
5 NetEraser technology, right?

6 A. Yes, sir.

7 Q. And Magenic was working with a Microsoft
8 product at that time, the Live Communication Server.

9 A. Yes, sir.

10 Q. And the purpose of that work, as you learned
11 it from Mr. Larsen, was to modify Microsoft's Live
12 Communication Server in order to add the VirnetX
13 patented technology to it, right?

14 A. No, sir.

15 Q. Would Mr. Larsen know that better than you
16 since he was directing it?

17 A. He probably -- he might have.

18 Q. All right. Well, Mr. Larsen will testify
19 later, and we'll get his testimony.

20 Now, the objective of the Magenic work,
21 though, was to try to implement your patented
22 technology. That was the objective, wasn't it?

23 A. That's -- that's a correct statement, sir.

24 Q. So let's look at DX3536. Let me know when you
25 have it.

1 A. I have it, sir.

2 MR. POWERS: Bring up the first, oh, six,
3 seven lines. That's perfect.

4 Q. (By Mr. Powers) This is a work order between
5 VirnetX and Magenic, and it's in 2006 --

6 A. Yes, sir.

7 Q. -- before you arrived?

8 A. Yes, sir.

9 Q. And so this is one of the things Kendall
10 Larsen, VirnetX's CEO, was managing and running before
11 you arrived?

12 A. Yes, sir, that's correct.

13 Q. Have you ever seen this document before?

14 A. I don't recall it, no, sir.

15 Q. Let's look at the next page and see if it
16 helps you recall.

17 MR. POWERS: There's a section, Chris, on
18 Page 2 that starts: Goals, deliverables, work plan, and
19 schedule. And let's take that all the way down to the
20 bullet points that are the second set of bullet points.

21 Oh, it's going to be hard to read, isn't
22 it?

23 Q. (By Mr. Powers) Can you read that, Mr. Munger?

24 A. Yes, sir.

25 Q. Okay.

1 MR. POWERS: And can the jury read that?
2 It's a little far off.

3 I will read it in the record so that it's
4 clear.

5 Q. (By Mr. Powers) Under project goal, it says,
6 quote, the goal of the project, in short, is to come up
7 with a solution for encrypted secure communication
8 stream between multiple messaging end points.

9 This will be accomplished by implementing a
10 first phase of a wheel-and-spoke architecture with
11 VirnetX at the center, connecting different corporate
12 architectures. This needs to be accomplished using as
13 simple a method as possible while utilizing VirnetX's
14 patents.

15 Do you see that?

16 A. Yes, sir.

17 Q. Do you understand that that was the goal, the
18 Magenic project, before you arrived, or is that just
19 something we have to rely on Mr. Larsen for?

20 A. This is almost a surprise to me, sir.

21 Q. So Kendall Larsen is the person who can answer
22 that?

23 A. Yes, sir.

24 Q. All right. Do you -- did you ever have a
25 discussion with Kendall Larsen as to why he was

1 attempting to modify Microsoft's Live Communication
2 Server and Office Communicator in order to use the
3 VirnetX patented technology?

4 A. There was no discussion about modifying a
5 Microsoft application.

6 Q. Well, you weren't there.

7 A. With me. The answer to that specifically with
8 me, sir.

9 Q. I'm talking about the period before you
10 arrived.

11 Did you ever ask Mr. Larsen, Kendall Larsen,
12 or did he tell you why he was trying, before you
13 arrived, to modify Microsoft's Office Communicator and
14 Live Communication Server in order to use VirnetX's
15 patented technology?

16 Did you hear anything from him about the
17 reason for that?

18 A. I'm looking for the word modify, but there was
19 no discussion about modify, sir.

20 Q. And those two products, Microsoft Office
21 Communicator 2005 and Live Communication Server 2005,
22 you understand that those are two products, which in
23 this lawsuit, VirnetX is saying infringed VirnetX's
24 patent back then.

25 True?

1 A. That's true, sir.

2 Q. And yet you have no explanation for why
3 Mr. Larsen, Kendall Larsen, is trying to modify those
4 products in order to use the VirnetX patents; you just
5 don't know.

6 Is that fair?

7 A. I'm sorry. I still have a problem with the
8 word modify.

9 But he had an effort to provide security
10 platforms for those, and that's -- that's my
11 understanding of what was going on.

12 Q. But you really don't know the answer, because
13 we'd have to ask Mr. Larsen for that?

14 A. I think so, yes, sir.

15 Q. All right. Now, let's talk a little more
16 about Gabriel. Actually, one quick question before we
17 get there.

18 On direct examination, you testified about a
19 company called Cambridge Strategy Management, right?

20 A. Strategic, yes, sir.

21 Q. Strategic management. Sorry.

22 And that was a company that SAIC hired to tell
23 them whether there was a business opportunity out there
24 in this space, true?

25 A. That's correct, sir.

1 Q. Cambridge Strategy Management -- or Strategic
2 Management didn't actually assess the quality of your
3 software and decide that that specific software had that
4 value, did it?

5 A. No, sir.

6 Q. All right. Now, let's move, then, to Gabriel.
7 In your direct examination, Mr. Cawley asked you why did
8 you continue development of Gabriel after you came to
9 VirnetX.

10 Do you recall that question and your answer?

11 A. Yes, sir.

12 Q. And you gave three answers, three reasons, the
13 first being so that you could have a secure domain name
14 service product, right?

15 A. Yes, sir.

16 Q. The second being to support licensing?

17 A. Yes, sir.

18 Q. And the third would be to support this
19 litigation?

20 A. That's correct, sir.

21 Q. In fact, weren't the priorities and the
22 reasons exactly the reverse in that order?

23 A. No, sir.

24 Q. Do you recall -- you say you remember the
25 Board of Directors, right?

1 A. Yes, sir.

2 Q. And the Board of Directors actually addressed
3 this precise issue, didn't they?

4 A. Yes, sir.

5 Q. Would you look at 3161, please, Exhibit 3161?
6 Tell me when you have it. Do you have it in
7 front of you?

8 A. Oh, yes, sir. I'm sorry.

9 Q. All right. Exhibit 3161 is a presentation to
10 the Board of Directors in March of 2008 of VirnetX,
11 right?

12 A. Yes, sir.

13 Q. That's after this litigation started, over a
14 year after, right?

15 A. Yes, sir.

16 Q. And you're a member of the Board of Directors
17 at this time, weren't you?

18 A. Yes, sir.

19 Q. And if you turn to Page 22 of the document,
20 there's a page that -- the title is Gabriel Technology
21 Thrust Objectives.

22 Do you see that?

23 A. Yes, sir.

24 Q. Now, the first stated purpose or objective is
25 to support IP licensing.

1 Do you see that?

2 A. Yes, sir.

3 Q. In fact, Gabriel has not been licensed to
4 anyone, has it?

5 A. No, sir.

6 Q. The second stated purpose, which you had put
7 last in your testimony, was embody patented methods to
8 support litigation.

9 That's the same way you're referring to it
10 here, wasn't it?

11 A. Yes, sir.

12 Q. And the third and last here, but your first,
13 was prepare technical product for providing direct
14 product and services to the public as appropriate.

15 Do you see that?

16 A. Yes, sir.

17 Q. So as of March of 2008, in terms of the
18 listing for Gabriel and Gabriel's objectives, having a
19 real product was third and last and only as appropriate.

20 True?

21 A. No, sir.

22 Q. Is that not what it says?

23 A. Oh, let me read what it says.

24 Yes, sir.

25 Q. Now, within VirnetX, you understood that the

1 purpose -- the primary purpose, actually, of the work
2 you were doing on Gabriel was to support this
3 litigation?

4 A. No, sir.

5 Q. You didn't?

6 Did you ever hear inside VirnetX the Gabriel
7 software being referred to as, quote, vaporware, close
8 quote?

9 A. No, sir.

10 Q. Never heard of it?

11 A. No, sir.

12 Q. Do you know what the phrase vaporware means?

13 A. Yes, sir.

14 Q. It means software that doesn't really exist,
15 that's just sort of appear to be software but doesn't
16 really exist.

17 Is that fair?

18 A. Yes, sir. That's a fair estimate in my
19 definition.

20 Q. Would you look at Exhibit 3260, please.

21 Let me know when you're there.

22 A. I'm there, sir.

23 Q. Exhibit 3260 is an internal e-mail within
24 VirnetX, isn't it?

25 A. Yes, sir.

1 Q. It's from a man named Gordon Warren to you and
2 other people in July of 2008, correct?

3 A. Yes, sir.

4 Q. July 2008 is a few months after the Board
5 meeting we just looked at in March of 2008, right?

6 A. Yes, sir.

7 Q. And Gordon Warren is an engineer at VirnetX,
8 isn't he?

9 A. Yes, sir.

10 Q. He's one of the people who's actually working
11 in the Gabriel software, right?

12 A. Yes, sir.

13 Q. And what he says is: Vic, group-shmoop --
14 with my apologies to the court reporter, that's
15 S-H-M-O-O-P -- it's all vaporware, with a little smiley
16 face at the end.

17 Do you see that?

18 A. Yes, sir.

19 Q. Now, you received this e-mail from Mr. Warren.

20 A. Yes, sir. I'm an addressee on it.

21 Q. So you knew that Mr. Warren in July of 1998
22 (sic) was saying as to Gabriel, it's all vaporware?

23 A. No, sir.

24 Q. Well, the subject of this e-mail is file
25 registry -- file share registry change working on

1 Gabriel software, right?

2 A. Yes, sir.

3 Q. All right. And you know Mr. Warren was
4 working on Gabriel at the time; that was his primary
5 job, right?

6 A. Yes, sir.

7 Q. And he's saying it's all vaporware?

8 A. I think he might be referring to some aspect
9 of the file share registry, which is not our total code,
10 sir.

11 Q. Okay. Now, when you were working on Gabriel
12 for VirnetX, you did nothing to determine whether
13 Gabriel will infringe somebody else's patents, do you?

14 A. Would you repeat the question?

15 Q. Certainly.

16 You're working on Gabriel as a possible
17 product, true?

18 A. Yes, sir.

19 Q. That's what you just said.

20 And you don't do anything to decide -- to
21 figure out whether Gabriel would infringe somebody
22 else's patents, do you?

23 A. No, sir. I haven't done that.

24 Q. And VirnetX doesn't have a policy of asking
25 anyone to do that, does it?

1 A. There's no written policy like that, no, sir.

2 Q. Or unwritten policy, is there?

3 A. Not that I know of, yes, sir.

4 Q. Now, let's look at Exhibit DX3259, please.

5 Let me know when you have it.

6 A. I have it in front of me, sir.

7 Q. Exhibit 3259 is an e-mail from you to Vic
8 Larson, one of your co-inventors, and Bob Short, one of
9 your co-inventors, and others in November of 2007,
10 right?

11 A. Yes, sir.

12 Q. And you're addressing a user's guide for
13 Gabriel as of -- in November of 2007, right?

14 A. Yes, sir.

15 Q. And you attached that user's guide that you
16 had reviewed and worked on, true?

17 A. That's true, sir.

18 Q. And one of the things this user's guide does
19 is stipulate the sign-in procedure when the developers
20 are going to work on Gabriel software, right?

21 A. That's correct, sir.

22 Q. So if you personally went to go work on the
23 software or when anyone else did, they would have to log
24 in to Gabriel using a password that had bene selected
25 for that purpose, true?

1 A. Yes, sir. It was actually to download the --
2 this was part of it, to download the software.

3 Q. And if you look at Page 13 of the document,
4 this is -- this is the actual Gabriel user's guide draft
5 as it existed in November of 2007?

6 A. Yes, sir.

7 Q. Which you attached to your e-mail?

8 A. Yes, sir.

9 Q. Now --

10 MR. POWERS: Chris, if you could pull up
11 from the text in between the two boxes all the way down
12 to the box -- to the last box.

13 Q. (By Mr. Powers) This was the log-in screen
14 that was used in the Gabriel development software at
15 that time, right?

16 A. Yes, sir. For about a two-week period, that's
17 a correct statement.

18 Q. And we've all used log-in screens where you
19 have to type in a user name and then a password, and
20 that's what you did in this process?

21 A. Yes, sir.

22 Q. And you personally logged in more than once to
23 this process using this password and user name?

24 A. Maybe twice, yes, sir.

25 Q. And others on the team did as well?

1 A. Yes, sir.

2 Q. And the user name that you used was VirnetX,
3 right?

4 A. Uh-huh.

5 Q. The name of the company?

6 And the password that was selected was
7 MS\$42009? (sic), question mark, correct?

8 A. Yes, sir.

9 Q. MS stood for Microsoft, didn't it?

10 A. Yes.

11 Q. \$4 meant are we going to get money from
12 Microsoft?

13 A. That's correct, sir.

14 Q. And 2009?, question mark, was stating when you
15 hoped to get money from Microsoft?

16 A. That's correct, sir.

17 Q. So your password that your development team
18 used for Gabriel was, are we going to get money from
19 Microsoft in 2009?

20 A. That's correct, sir.

21 Q. And is it still your testimony that the
22 primary purpose of Gabriel wasn't linked to this
23 litigation?

24 A. That's a correct statement, sir.

25 Q. Despite the fact that the password was

1 directly linked to this litigation?

2 A. Yes, sir.

3 Q. All right. Let's talk about the dates on
4 which you had the ideas for the claimed inventions that
5 are in this case.

6 You understand that's a concept that we're
7 calling conception?

8 A. Yes, sir.

9 Q. Have you heard that term before?

10 A. Yes, sir.

11 Q. And conception is when you have the idea for
12 what you later claim to be your invention?

13 A. Yes, sir.

14 Q. Now, did you ever tell Kendall Larsen what
15 those dates were for those patents-in-suit?

16 A. I can't remember.

17 Q. Let me show you Exhibit DX3428.

18 Let me know when you have it.

19 A. 3428, I have it, sir.

20 Q. Exhibit 3428 is a set of answers that VirnetX
21 gave under oath to questions that Microsoft asked them
22 in this litigation.

23 Do you understand that?

24 A. Yes, sir.

25 MR. POWERS: Your Honor, at this point,

1 would it be appropriate to have the Court instruct the
2 jury what an interrogatory is, or I can ask the witness
3 the question but --

4 THE COURT: Yes, I can do that.

5 Ladies and Gentlemen -- or Ladies of the
6 Jury, an interrogatory is a written question that is
7 sent to the other side during the course of the pretrial
8 proceedings where they provide a sworn answer to those
9 questions.

10 You may proceed.

11 MR. POWERS: Thank you, Your Honor.

12 If we can dim the lights again. Thank you.

13 Q. (By Mr. Powers) Now, one of the questions that
14 we asked VirnetX -- that Microsoft asked VirnetX was
15 Question 6, which starts at Page 5 of the document.

16 Let me know when you're there.

17 And it says: Separately, for each claim of
18 each of the patents-in-suit, state the date in which the
19 claimed inventions were conceived.

20 And you understand that's a question of when
21 you had the idea, right?

22 A. Yes, sir.

23 Q. All right.

24 MR. POWERS: And, Chris, why don't you
25 bring up the last -- let's bring up the whole -- the

1 whole answer to that.

2 Q. (By Mr. Powers) The whole first paragraph is a
3 bunch of objections, and the last paragraph is the
4 answer, and it says: VirnetX responds that the
5 inventions claimed in all of the patents-in-suit were
6 conceived no later than September 23, 1999.

7 Do you see that?

8 A. I see that, sir.

9 Q. And September 23rd, 1999 is the date of that
10 train ride that you testified about in direct
11 examination, right?

12 A. Yes, sir.

13 Q. Now, if you go two pages in, to No. 9, you see
14 that the person who verifies that those answers are true
15 is Kendall Larsen.

16 Do you see that?

17 A. Yes, sir, I do.

18 Q. Now, Kendall Larsen wasn't actually with you
19 on that train ride, was he?

20 A. No, sir.

21 Q. He doesn't know of his personal knowledge when
22 any of the inventions were made, does he?

23 A. No, sir.

24 Q. He wasn't there.

25 A. He wasn't there.

1 Q. So did you tell Kendall Larsen the information
2 that he verified under oath that all the inventions were
3 made in September of 1999?

4 A. No, sir.

5 Q. In fact, the statement in Exhibit 3428 that
6 all the inventions and all the claims were conceived no
7 later than September 23rd, 1999, that's not true, is it?

8 A. I don't believe that's true.

9 Q. In fact, one of the claim requirements for the
10 '135 is a secure target website, right?
11 '135 patent, if you want to look at that, I'd be happy
12 to get it.

13 A. I beg your pardon, sir?

14 Q. Do you need the patent in front of you to do
15 that?

16 A. Yeah. You're looking at the '135?

17 Q. The '135.

18 A. I can probably pull it up.

19 Q. The '135 patent was in the original binder
20 being used with Counsel at Exhibit 3, I believe.

21 Yes, Exhibit 3.

22 A. Well, I've also got it at 120, but there's
23 another copy that's here in a couple of places.

24 Q. There's a lot of copies of that patent in this
25 courtroom.

1 A. Yes, sir.

2 Q. So using Exhibit 3, which is the one that used
3 in your direct examination, what -- what are the
4 requirements of the claims -- and let's just take, for
5 example, Claim 10 -- is a secure target website.
6 Sorry. Claim 1.

7 A. Claim 1, sir?

8 Q. Yes. If you look at Claim 1 --

9 MR. POWERS: Let's bring it up.

10 Q. (By Mr. Powers) -- do you see secure target
11 website down there in the middle of the third step?
12 It's highlighted on the screen if you -- if you want --

13 A. Yes, sir. I see Claim 3 on this -- Step 3 in
14 Claim 1, yes, sir.

15 Q. And that step in Claim 1 of the '135 patent
16 includes a requirement of this secure target website?

17 A. Yes, sir.

18 Q. Now, that concept of a secure target website
19 had not been conceived as of September of 1999, right?

20 A. Yes, sir. With that definition, the
21 triggering was looking for secure target website.

22 Q. Let me make sure I understand your testimony.
23 Are you saying that, yes, secure target
24 website was conceived on September 23rd, 1999?

25 A. It was -- it was conceived -- the only thing

1 that was conceived on the 23rd was the revelation of the
2 triggering using DNS.

3 Between then and the time we applied for this
4 patent, there would have been a continuing unfolding of
5 the methods necessary to put in a patent.

6 Q. So let's be -- let's make sure the testimony
7 is clear.

8 You said the only thing that was conceived on
9 September 23rd was that secure DNS; the rest came later?

10 A. I would think that -- again, there might have
11 been a couple of things, but I would think that the bulk
12 of the methods and our understanding of how to do it
13 would have evolved over the next three months, yes, sir.

14 Q. And when you say would have evolved over the
15 next three months, you mean were not conceived on
16 September 23rd, 1999?

17 A. That's correct, sir.

18 Q. All right. And so as to the bulk of the '135
19 claims, Mr. Larsen's sworn statement in the
20 interrogatory response was not true?

21 A. That's correct, sir.

22 Q. All right. And it's also not true for the
23 '180 patent, is it?

24 A. Going back to the 23rd?

25 Q. Right.

1 A. Yes, sir, that's also correct.

2 Q. All right. Now, Victor Larson, not Kendall
3 Larsen now -- Victor Larson was one of your co-inventors
4 at SAIC, correct?

5 A. That's a correct statement, sir.

6 Q. And one of the things that you and Victor
7 Larson and Bob Short discussed, three -- three of the
8 inventors, was the relationship between the technology
9 called SIP and your technology, right?

10 A. There were discussions about it, yes, sir.

11 Q. And could please tell the jury what SIP is?

12 A. Session Initiation Protocol.

13 Q. And Session Initiation Protocol is a
14 technology that you understand or thought was being used
15 by Microsoft, true?

16 A. Yes, sir.

17 Q. All right. Now, could you turn to Exhibit
18 3257, please?

19 Let me know when you have it.

20 A. All right, sir.

21 Q. Exhibit 3257 is a collection of two e-mails
22 within SAIC in the November of 2005 time period, right?

23 A. Yes, sir.

24 Q. And you were still at SAIC at this time, as
25 was Victor Larson and Bob Short?

1 A. That's correct, sir.

2 Q. And if go -- then there's two e-mails here.

3 MR. POWERS: Let's bring up, please,
4 Chris, first the bottom one.

5 Can the jury see that one? The type is a
6 little hard to see, okay?

7 I can't see it on the screen either, so
8 I'll read it.

9 Q. (By Mr. Powers) First, Mr. Munger, you were
10 copied on this e-mail from Bob Short in November of
11 2005, weren't you?

12 A. Yes, sir.

13 Q. And the subject of the e-mail is SIP Secure.
14 Do you see that?

15 A. Yes, I do, sir.

16 Q. Now, you know that SIP Secure referred to the
17 use of SIP, which is this Session Initiation Protocol,
18 plus an additional type of technology, for example, TLS
19 or SSL?

20 A. Yes, sir.

21 Q. And TLS and SSL are just two different ways of
22 doing -- making a communication secure, right?

23 A. Yes, sir.

24 Q. And you didn't invent those and you don't
25 claim that those infringe, do you?

1 A. It's not clear that they infringe or not.

2 Q. You don't have an opinion that they do. You
3 haven't concluded that, have you?

4 A. No. I have not looked into it, sir.

5 Q. Okay. Now, Mr. Short, your co-inventor, says
6 to you and others in November of 2005, quote, I find
7 myself losing the bubble on what distinguishes us from
8 SIPS.

9 Do you see that?

10 A. Yes, sir.

11 Q. So, Mr. Short, your co-inventor, is saying to
12 you, I can't figure out why we're any different or
13 better than this SIP Secure, true?

14 A. That's what the e-mail says, yes, sir.

15 Q. All right. And if we go to the e-mail above
16 it, it's an e-mail from Victor Larson, your co-inventor,
17 back to Bob Short, responding to his earlier e-mail,
18 right?

19 A. Yes, sir.

20 Q. And Victor Larson, one of your co-inventors,
21 says, quote: I did not come away from the
22 Thursday/Friday meetings with a strong feeling that our
23 patent provided any amount of protection against
24 reasonably secure approaches for SIP, parens, i.e., TLS,
25 close parens, close quote.

1 Do you see that?

2 A. Yes, sir.

3 Q. So that's your co-inventor saying our patents
4 don't protect against that technology, SIP plus TLS,
5 true?

6 A. Yes, sir, he had a strong feeling.

7 Q. Okay. And you didn't write back to him
8 saying, well, no, our patents do cover that, did you?

9 A. No, sir.

10 Q. All right. And you understand that the
11 products you say infringe here use SIP plus TLS.

12 A. I understand that, yes, sir.

13 Q. The very same products that your co-inventor
14 said your patents don't protect are the same products
15 which are now -- you're saying do -- are covered by the
16 patent.

17 A. That's what we're saying, yes, sir.

18 Q. Okay. Now, let's talk a little bit about
19 Kendall Larsen.

20 He -- at VirnetX, he's the person who
21 negotiates the key contracts, isn't he?

22 A. Yes, sir.

23 Q. Including licenses or anything else. That's
24 part of his job.

25 A. Yes, sir.

1 Q. And at this point, all of the attempts that
2 have been made at VirnetX to license either the patents
3 or the technology has not resulted in any license, true?

4 A. Yes, sir.

5 MR. POWERS: Pass the witness, Your
6 Honor.

7 THE COURT: All right. Redirect?

8 MR. CAWLEY: Thank you, Your Honor. Just
9 a few questions.

10 REDIRECT EXAMINATION

11 BY MR. CAWLEY:

12 Q. Mr. Munger, let's talk about this password,
13 MS4\$2009, question mark, that you showed us in
14 Defendant's Exhibit 3259.

15 What document was that in again?

16 A. That was in a first attempt to try to set up
17 what steps you take to install Gabriel software and
18 download the domain name into that software.

19 Q. Is that an internal document to VirnetX, or
20 did it go out into the world?

21 A. Well, sir, there was only five of us that
22 would have seen that document.

23 Q. And was that document written and who used
24 that password in that document?

25 A. Dr. Vic Larson told me that he did that

1 password.

2 Q. Okay. So he put that password in there,
3 didn't send it to anybody outside the company.

4 Was the lawsuit already filed by then, this
5 lawsuit?

6 A. Yes, sir.

7 Q. And was this lawsuit at that time set for
8 trial, not now but in the year 2009?

9 A. Yes, sir.

10 Q. How many employees are there at VirnetX?

11 A. There's 12 employees.

12 Q. Twelve employees.

13 And would you say that they -- at the time
14 Mr. Larson used that password were all anxious about how
15 this lawsuit is going to turn out?

16 A. Very.

17 Q. How long was that password in that document?

18 A. Maybe two weeks.

19 Q. Two weeks.

20 You testified, when I was asking you questions
21 before, about your delivery of the NetEraser prototype
22 to In-Q-Tel and the CIA. And I asked you if you knew
23 whether or not the CIA had actually used your invention.

24 Do you remember that?

25 A. Yes, sir.

1 Q. And you said, I believe, you didn't know one
2 way or the other.

3 A. Yes, sir.

4 Q. Then on cross-examination, you were just shown
5 some deposition testimony where you said you didn't know
6 if the CIA was using your invention; isn't that right?

7 A. That's correct.

8 Q. Is that inconsistent in any way in your mind?

9 A. No, sir.

10 Q. You don't know if they're using it, and you
11 don't know if they're not. Is that the truth?

12 A. That's the truth, sir.

13 Q. Okay. You were asked some questions about
14 several different kinds of prior art, https, DVPN, and
15 Aventail.

16 First of all, you told us before that you
17 helped work on your patents. So are you generally
18 familiar with the phrase prior art?

19 A. Yes, sir.

20 Q. And do you understand that prior art means
21 something that was written about or used or existed
22 before a certain date?

23 A. Yes, sir.

24 Q. So it doesn't really tell you anything about
25 whether a particular technology used your idea just

1 because it's, quote, prior art, does it?

2 A. No, sir.

3 Q. Well, let's talk about the things that you
4 were -- were asked about that were called prior art,
5 meaning only that they were around before your
6 invention.

7 You testified that https was fast and secure,
8 but would it have solved the needs of the CIA?

9 A. No, sir.

10 Q. Why not?

11 A. Because it only went from a client to a server
12 and wasn't flexible enough to route to other machines,
13 sir.

14 Q. All right. You were asking about a piece of
15 prior art called DVPN.

16 Do you remember that?

17 A. Yes.

18 Q. You were asked several questions about that.

19 And do you remember this morning that
20 Microsoft's lawyer in the opening statement told this
21 jury that in February of 1998, there was a meeting in
22 Annapolis, Maryland, hosted by DARPA, where DVPN was
23 discussed?

24 Do you remember that?

25 A. Yes, sir.

1 Q. And do you remember that Microsoft's lawyer
2 told this jury that you were at that meeting?

3 Did you hear that?

4 A. Yes, sir.

5 Q. Mr. Larson, is that true?

6 A. Well --

7 Q. Mr. Munger, is that true?

8 A. I was not at that meeting, sir.

9 Q. Are you confident about that?

10 A. Yes, sir.

11 Q. Have you had an opportunity within today to
12 review an attendee list for that meeting?

13 A. Yes, sir, I did.

14 Q. And is that list a Defendant's exhibit marked
15 by the Defendants as an exhibit in this case and
16 admitted into evidence, Exhibit 3011?

17 A. Yes, sir.

18 Q. Is your name on that list?

19 A. No, sir.

20 Q. Another piece of prior art you were asked
21 about is Aventail.

22 Do you know if ANX was using Aventail in May
23 of 2000?

24 A. No, sir.

25 Q. And a few minutes ago, you were asked a lot of

1 questions that would seem to be trying to get you to
2 agree that Mr. Larsen at VirnetX had tried to modify the
3 Microsoft Live Communications Server product.

4 Do you remember that?

5 A. Yes, sir.

6 Q. Let's go over that again, because I know you
7 testified about it in your direct examination.

8 Was there a period of time when Mr. Larsen had
9 formed the company VirnetX, but you still worked at
10 SAIC?

11 A. Yes, sir.

12 Q. And did he hire you and SAIC to do something?

13 A. Yes, sir.

14 Q. What did he hire you to do?

15 A. He hired us to recommend to him a -- how to
16 technically develop a product that had been updated from
17 our previous experience.

18 Q. And what would that product work with?

19 A. It would work with any application.

20 Q. And, specifically, did you explore the
21 possibility, on behalf of VirnetX, of it working with
22 Microsoft Live Communications Server?

23 A. Yes, sir.

24 Q. Were you going to modify the Live
25 Communications Server?

1 A. No, sir.

2 Q. Were you instead going to make a product that
3 would work along with it to provide automated security?

4 A. That's a correct statement, sir.

5 Q. But in the course of exploring the possibility
6 of doing that, what did you begin to suspect?

7 A. I began to suspect that what Magenic was
8 doing -- this is after I got there -- that they -- they
9 weren't making progress and they might not have
10 understood technically the right approach to go forward
11 with, sir.

12 Q. All right. And, finally, Mr. Munger, you
13 testified both on the questions I asked you, and then
14 you were asked about it again by Microsoft lawyers, that
15 you approached venture capitalists about raising money
16 for your invention and they said no.

17 You approached co-developers about
18 co-developing, and they said no. SAIC said no. Various
19 government agencies said no.

20 Mr. Munger, in the face of all that, do you
21 still believe in your invention?

22 A. Yes, sir.

23 Q. Can you explain?

24 A. What -- what this is going to provide is an
25 easy way for any machine to connect to any other machine

1 safely. And I also think that the market is now here
2 with handheld smart phones that are becoming computers
3 that we have on our hip; people are going to reach to
4 their homes; that this is -- it's finally become a
5 technology whose time has arrived.

6 MR. CAWLEY: No more questions, Your
7 Honor.

8 THE COURT: Thank you. Any recross?

9 MR. POWERS: Nothing further, Your Honor.

10 THE COURT: All right. Thank you.

11 You may step down, Mr. Munger.

12 All right. Ladies and Gentlemen --
13 Ladies of the Jury, it's going to take me a while to
14 break that habit this week.

15 It's 20 minutes till 5:00. I think we're
16 going to go ahead and recess for the day. We'll start
17 back in the morning at 9:00 o'clock. So get a good
18 night's rest tonight.

19 Please try to be here a few minutes
20 before 9:00 so that we can get started, hopefully,
21 promptly at 9:00.

22 Please remember my instructions this
23 evening. Don't discuss the case among yourselves or
24 with anyone else. Don't make any independent
25 investigation. Don't read anything, if you should see

1 anything in a newspaper or on television.

2 So you are recessed at this time. You
3 can go to the jury room and head on to your homes.

4 COURT SECURITY OFFICER: All rise for the
5 jury.

6 THE COURT: All right. Members of the
7 Jury, if you would, please be sure to leave your
8 notebooks and your notepads in the jury room. The court
9 security officer will secure all those and get them back
10 to you tomorrow.

11 (Jury out.)

12 THE COURT: All right. Very well.

13 Is there anything further from the
14 Plaintiffs?

15 MR. CAWLEY: No, Your Honor.

16 THE COURT: From the Defendants?

17 MR. POWERS: No, Your Honor.

18 THE COURT: All right. We're going to be
19 in recess. It's 4:40. I'm going to ask everyone to
20 remain in the courtroom for about five minutes and allow
21 the jury to get to their cars to the elevators ahead of
22 you.

23 So, Ms. Ferguson, you're in charge as far
24 as dismissing everyone.

25 Be in recess.

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

COURT SECURITY OFFICER: All rise.

(Court adjourned.)

* * * * *

CERTIFICATION

I HEREBY CERTIFY that the foregoing is a true and correct transcript from the stenographic notes of the proceedings in the above-entitled matter to the best of my ability.

/s/_____
SUSAN SIMMONS, CSR
Official Court Reporter
State of Texas No.: 267
Expiration Date: 12/31/10

Date

/s/_____
JUDITH WERLINGER, CSR
Deputy Official Court Reporter
State of Texas No.: 731
Expiration Date: 12/31/10

Date

EXHIBIT F3

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

1			
2			
3	VIRNETX	*	Civil Docket No.
4		*	6:07-CV-80
5	VS.	*	Tyler, Texas
6		*	March 9, 2010
7	MICROSOFT CORPORATION	*	9:00 A.M.

TRANSCRIPT OF JURY TRIAL
BEFORE THE HONORABLE JUDGE LEONARD DAVIS
UNITED STATES DISTRICT JUDGE

APPEARANCES:

12	FOR THE PLAINTIFFS:	MR. DOUGLAS CAWLEY
13		MR. BRADLEY CALDWELL
14		MR. JASON D. CASSADY
15		MR. LUKE MCLEROY
16		McKool-Smith
17		300 Crescent Court
18		Suite 1500
19		Dallas, TX 75201
20		MR. ROBERT M. PARKER
21		Parker, Bunt & Ainsworth
22		100 East Ferguson
23		Suite 1114
24		Tyler, TX 75702

APPEARANCES CONTINUED ON NEXT PAGE:

22	COURT REPORTERS:	MS. SUSAN SIMMONS, CSR
23		Ms. Judith Werlinger, CSR
24		Official Court Reporters
25		100 East Houston, Suite 125
		Marshall, TX 75670
		903/935-3868

(Proceedings recorded by mechanical stenography,
transcript produced on CAT system.)

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

APPEARANCES CONTINUED:

FOR THE DEFENDANT: MR. MATTHEW POWERS
MR. JARED BOBROW
MR. PAUL EHRLICH
MR. THOMAS KING
MR. ROBERT GERRITY
Weil Gotshal & Manges
201 Redwood Shores Parkway
5th Floor
Redwood City, CA 94065

MS. ELIZABETH WEISWASSER
MR. TIM DeMASI
Weil Gotshal & Manges
767 Fifth Avenue
New York, NY 10153

MR. DANIEL BOOTH
Weil Gotshal & Manges
700 Louisiana
Suite 1600
Houston, TX 77002

MR. RICHARD SAYLES
MR. MARK STRACHAN
Sayles Werbner
1201 Elm Street
4400 Renaissance Tower
Dallas, TX 75270

MR. ERIC FINDLAY
Findlay Craft
6760 Old Jacksonville Highway
Suite 101
Tyler, TX 75703

* * * * *

P R O C E E D I N G S

(Jury out.)

COURT SECURITY OFFICER: Please rise.

THE COURT: Please be seated.

All right. I understand the parties have

1 a matter or two before we bring the jury in.

2 MR. SAYLES: Yes, Your Honor. If it
3 please the Court, Dick Sayles for Microsoft.

4 Your Honor, this afternoon a witness to
5 be called is Mr. Brett Reed, who is the Plaintiff's
6 damages expert. I'll be cross-examining him.

7 And one of the issues related to his
8 testimony is some approximately 80 exhibits to which
9 Microsoft cannot agree to admissibility.

10 And, Your Honor, in keeping with the --
11 the spirit of how matters such as this are handled in
12 this district, we have agreed in every respect where we
13 can agree.

14 We're not asking that they establish a
15 business records predicate or any sort of a thing like
16 that. These objections to these particular exhibits go
17 to the -- the heart of their damage model.

18 And the nature of the exhibits is the
19 same objections that I brought forward in the motion to
20 strike Mr. Reed and -- and that was denied at pretrial,
21 and -- and the motion in limine and the motion
22 concerning the entire market value, and those were all
23 denied.

24 And having the experience of -- of been
25 around for a while, I know that a pretrial ruling of

1 that nature doesn't preserve anything. Microsoft is
2 very intent on preserving its position and its
3 objections with regard to these particular damages that
4 it believes are irrelevant financial data not tied to
5 the demand for the technology at issue.

6 The -- the problem is that there are some
7 80 of these. And if they were handled one by one and
8 tendered by the Plaintiff and objected to on a
9 one-by-one basis, it would obviously take a long time to
10 do that.

11 I have spoken with Jason Cassady for the
12 Plaintiff at some length. We have prepared lists of the
13 exhibits that they intend to tender in evidence. And
14 when they do, we have written out what our objections to
15 those exhibits are. And we in no way wish to diminish
16 the importance of those objections.

17 We do not wish to waive those objections,
18 but we do want to suggest to the Court or discuss with
19 the Court a convenient and realistic manner in which to
20 handle those important objections to these exhibits.

21 And similarly, the Plaintiffs have
22 properly disclosed to us last night demonstratives that
23 they intend to use with Mr. Reed. And as you might
24 imagine, those demonstrative aids are based upon the
25 underlying documents to which we object, and, therefore,

1 we have the same objection to those demonstratives.
2 And we have prepared numbered sets of those. And I
3 don't think this morning is necessarily the time to go
4 into this in great detail, although if that were the
5 Court's wish, we're prepared to.

6 But I wanted to speak with the Court this
7 morning to offer as a possible solution that the
8 Plaintiff has agreed that they will tender their
9 exhibits in a written list to which we have our written
10 objections, which we can provide to the Court in advance
11 of this afternoon and obtain a ruling.

12 There are only two exhibits which we have
13 separated out of that that have unique, special
14 objections to them. And those would not take long.

15 But I wanted to bring that up with the
16 Court, because I expect we want to move this case along.
17 And when we get to Mr. Reed this afternoon, I know that
18 Your Honor will want to keep things moving. And so
19 that's the issue.

20 And if -- if the Court would indulge us
21 and permit us to handle it in a manner that I have
22 suggested, we'll work together to do that.

23 THE COURT: And you're basically wanting
24 to make a record on these; is that --

25 MR. SAYLES: I definitely want to make a

1 record. We do -- we would really, of course, like you
2 to sustain our objections.

3 I will say, as I argued in the pretrial
4 motions, our objections go to the heart of their damage
5 model, and we do want to make a record. I mean, it's
6 not like we want to make a record and, therefore, I am
7 not intent and serious about the objections.

8 But, yes, we do want to make a record.
9 That's correct.

10 THE COURT: Response?

11 MR. CASSADY: Your Honor, Mr. Sayles
12 correctly stated that these are all subject to motions
13 that were filed, either motions to strike or motions in
14 limine that the Court has already ruled on in the
15 Plaintiff's favor.

16 We have no objection to putting these
17 exhibits in -- in a list format, such as Mr. Sayles
18 suggested, so that the Court can rule on these in groups
19 and, hopefully, alleviate the burden of running through
20 these 80-some-odd exhibits on a one-by-one basis.

21 In general, I'll just state for the
22 Court, these are documents such as licenses, Microsoft's
23 financial data, and summaries of that financial data.

24 So as Mr. Sayles said, this does go to
25 the core of VirnetX's damages case, and I think the

1 rulings that the Court has already made on the motions
2 to strike and motions in limine go straight to these
3 documents.

4 MR. SAYLES: Indeed they do, Your Honor.
5 But as I say, I've learned the hard way that that
6 doesn't preserve anything.

7 THE COURT: Right. I think what I would
8 like to do on these is when we get to Dr. Reed or
9 before -- even before we get to him, I'd like to just
10 hear a little bit of testimony and get a little deeper
11 into what these documents are. The Court is aware of
12 the -- I think it's Resneck -- ResNet (sic) case out of
13 the Fifth Circuit.

14 MR. CASSADY: ResQNet.

15 THE COURT: ResQNet, yeah, that's it.
16 That -- and I'd like to hear a little argument on that.
17 And I understand Judge Folsom has a new opinion out.
18 Anyway, I'd just like to just delve into it a little
19 deeper and give it -- give it one more look. And I'll
20 consider your objections at that time.

21 MR. SAYLES: All right.

22 THE COURT: And I might give the jury a
23 little extra time for lunch today, and we might --
24 might -- we can probably do it in 30 minutes, don't you
25 think?

1 MR. SAYLES: Yes, Your Honor, I do think
2 so.

3 MR. CASSADY: I have no problem with
4 that, Your Honor.

5 MR. SAYLES: And, Judge, if I may, this
6 is just for my personal information.

7 I'm going to be handling this witness,
8 and, naturally, if there are objections when the witness
9 is testifying in front of the jury, I will make the
10 objections.

11 But with regard to presenting Your Honor
12 with legal arguments outside the presence of the jury
13 related to the admissibility of these documents, may I
14 have assistance from my team in doing so?

15 THE COURT: Yes, you may.

16 MR. SAYLES: All right.

17 THE COURT: All right. What else before
18 we bring the jury in?

19 MR. BOBROW: Just a brief matter, Your
20 Honor, if I may.

21 First of all, we have reached agreement
22 with the Plaintiff on the further admissibility of four
23 more exhibits for Defendant's exhibit list.

24 If I may --

25 THE COURT: Can we just bring those up in

1 front of -- we'll take those up in front of the jury
2 once they come in.

3 MR. BOBROW: All right. And then the
4 second issue is, is that last night we filed a bench
5 memo on the Dynamic VPN issue.

6 As you've heard, Dynamic VPN, Microsoft's
7 prior art in this case that invalidates these patents,
8 we have been unable to meet and confer process to
9 resolve the Plaintiff's objections to a number of
10 Dynamic VPN exhibits.

11 My sense is, is that there will be
12 testimony on Dynamic VPN probably on Wednesday or
13 Thursday of this week, and we simply wanted to alert the
14 Court to that; number one, that we filed that memo and,
15 number two, that it will need to be resolved as that
16 evidence, we hope, will be coming in in our case.

17 THE COURT: All right. We'll take that
18 up either late this afternoon or perhaps in the morning.

19 Remind me about it again at the end of
20 the day.

21 MR. BOBROW: Thank you, Your Honor.

22 THE COURT: Anything further?

23 MR. McLEROY: Your Honor, when should we
24 offer our list of exhibits that were admitted?

25 THE COURT: As soon as the jury comes in,

1 I'll give you an opportunity to do that.

2 Anything further?

3 MR. CAWLEY: No, Your Honor.

4 THE COURT: All right. Bring the jury
5 in, please.

6 COURT SECURITY OFFICER: All rise for the
7 jury.

8 (Jury in.)

9 THE COURT: Please be seated.

10 Good morning, Ladies of the Jury. Ready
11 to get going?

12 All right. Very well.

13 Mr. Cawley -- let's see. Yes,
14 Mr. Cawley, you may call your next witness.

15 MR. CAWLEY: Thank you, Your Honor.
16 Do we want to introduce the exhibits first?

17 THE COURT: Yes. We will do exhibits
18 first. Does Plaintiff have any additional exhibits to
19 offer this morning?

20 MR. McLEROY: No additional exhibits,
21 Your Honor, but we do have a list of the exhibits
22 admitted yesterday for the Court.

23 THE COURT: Okay. Very well.

24 MR. McLEROY: May I approach?

25 THE COURT: You may provide those to,

1 Ms. Ferguson. Thank you for preparing that.

2 MR. McLEROY: You're welcome.

3 THE COURT: Does Microsoft have any
4 exhibits it wishes to offer?

5 MR. POWERS: Yes, Your Honor. We have, I
6 believe, four that we wish to offer this morning as to
7 which there's no objection. We have a similar list as
8 to what was admitted yesterday.

9 May I approach?

10 THE COURT: Now, the similar list you
11 have, are those the exhibits that were admitted
12 yesterday?

13 MR. POWERS: Exactly.

14 THE COURT: Okay. Now, what are the four
15 exhibits you wish to offer today.

16 MR. BOBROW: Thank you, Your Honor.

17 The four exhibits are Defendant's
18 Exhibits 3032, 3066, 3253, and 3577.

19 THE COURT: Okay. Any objection?

20 MR. McLEROY: No, Your Honor, I don't
21 believe we do.

22 THE COURT: All right. Be admitted.
23 All right. And you may bring the list up, Mr. Powers.

24 MR. POWERS: Thank you, Your Honor.

25 THE COURT: All right. Mr. Cawley, you

1 may call your witness.

2 MR. CAWLEY: Thank you, Your Honor.

3 As this next witness, the Plaintiff,
4 VirnetX, would call to the stand Dr. Bob Short.

5 THE COURT: All right.

6 MR. POWERS: Your Honor, may I approach
7 with the --

8 THE COURT: Yes, you may.

9 ROBERT D. SHORT, III, Ph.D., PLAINTIFF'S WITNESS,

10 PREVIOUSLY SWORN

11 DIRECT EXAMINATION

12 BY MR. CAWLEY:

13 Q. Would you please introduce yourself to the
14 jury please, sir?

15 A. My name is Robert Dunman Short, III.

16 Q. Mr. Short, I want to make sure that we are
17 able to hear all of your testimony, so I think, as we've
18 seen from yesterday, don't get too close to that
19 microphone, or it starts making popping noises. But
20 please make sure you're speaking more or less into it.

21 Why are you here?

22 A. I'm one of the co-inventors on the patents in
23 this case.

24 Q. What did you invent?

25 A. We invented a way to make it much easier for

1 the average user to have a safe connection on the
2 internet.

3 Q. Is your invention important?

4 A. Yes, sir, I believe it is.

5 Q. Why do you say that?

6 A. There's lots of information going across the
7 internet. Some of it is not very important. A lot of
8 it is very important. People's bank account
9 information, credit card information, family pictures.
10 And there's a lot of bad people out there trying to get
11 that information and -- and use it.

12 Q. So are you listed as an inventor on the two
13 patents in this case, along with Mr. Munger, that we
14 heard from yesterday?

15 A. Yes, sir.

16 Q. And were there others on your team who were
17 also inventors?

18 A. Yes, sir.

19 Q. Who were they?

20 A. We had Dr. Vic Larson and Mr. Mike Williamson
21 and Dr. Doug Schmidt.

22 Q. Okay. Which of those people worked for this
23 company, the Plaintiff in this lawsuit, VirnetX?

24 A. Four of the five. There's Gif and myself and
25 Vic Larson and Mike Williamson.

1 Q. Well, will your other inventors be here to
2 testify in Court?

3 A. No, sir.

4 Q. Why is that?

5 A. We had pretty limited time, so I think that's
6 the reason.

7 Q. All right. Where do you live?

8 A. I live in Loudon County, Virginia, outside of
9 Washington, D.C.

10 Q. Are you married?

11 A. Yes, sir. 32 years now.

12 Q. Okay. And is your wife here?

13 THE COURT: Mr. Cawley, excuse me. This
14 might be a good time for me just to explain to the
15 ladies of the jury that prior to trial, both sides gave
16 me an estimate of how much time they thought the case
17 would take. And then I told them -- arrived at an
18 amount of time, a number of hours that they had to
19 present their case.

20 So both sides are operating under some
21 time constraints, which will make the trial shorter for
22 you and, hopefully, keep them more focused. But when
23 the witness referred to a shortage of time, I wanted you
24 to understand where that came from.

25 So each side's operating under that same

1 constraint.

2 Excuse me, Mr. Cawley. I just wanted to
3 get that in.

4 MR. CAWLEY: Thank you, Your Honor. I
5 appreciate that clarification.

6 Q. (By Mr. Cawley) You say you're married. Is
7 this your wife here with you in the Court today?

8 A. Yes, sir.

9 Q. And you have children?

10 A. We have four children and two grandchildren.

11 Q. Did you go to college?

12 A. Yes, sir.

13 Q. Could you tell us about the schools that you
14 went to and the degrees that you got?

15 A. I started my -- my education at Virginia Tech.
16 I studied electrical engineering. Received a degree in
17 1974, a bachelor's degree.

18 I stayed there for another year of study in
19 applied mathematics, received a master's in applied
20 mathematics there.

21 Then I went on to Purdue University, which is
22 in Indiana, and studied electrical engineering, where I
23 received a Ph.D. in 1978.

24 Q. So you got your doctorate or your Ph.D. in
25 1978?

1 A. Yes, sir.

2 Q. So at that time, I guess, at least as people
3 refer to it in your field, you became Dr. Short.

4 What did you do after you got your Ph.D.?

5 A. I went to a company called Sperry Corporation
6 in Massachusetts.

7 Q. What kind of company was Sperry?

8 A. Sperry was a multi-division company that had a
9 fairly broad area that they worked in. For example,
10 they had one division that did sonar systems for
11 submarine warfare, radar systems. And there's another
12 one you may have heard of, Sperry-Univac, which is one
13 of the very early computer-makers.

14 And then there was Sperry New Holland -- you
15 may have heard of that -- which made farm equipment.

16 Q. What did you do at Sperry?

17 A. My first project at Sperry, I was at the
18 Corporate Research Center, and I was working on some
19 advanced methods for detecting, identifying, and
20 tracking Soviet submarines.

21 Q. Soviet submarines?

22 A. Yes, sir.

23 Q. How long did you stay at Sperry Corporation?

24 A. That was till -- about nine years, I believe.

25 Q. Nine years?

1 What did you do after you left Sperry?

2 A. I went to a company called ARCO Power
3 Technologies.

4 Q. What does ARCO do?

5 A. ARCO you may know better as
6 Atlantic-Richfield. It's an oil and gas company, and
7 they had a subsidiary called ARCO Power Technologies
8 that I worked for.

9 And what we did, we were working on some
10 pretty advanced radar techniques for looking over the
11 polar cap for incoming Soviet ballistic missiles. This
12 was during the Cold War.

13 Q. So you were developing radar systems that
14 would detect Soviet missiles in the event of an attack?

15 A. Yes, sir.

16 Q. Now, is it fair to say that your work at both
17 of these companies, Sperry and ARCO, had mostly military
18 applications?

19 A. Yes, that's right.

20 Q. When did you leave ARCO?

21 A. I left ARCO probably in the mid-'90s, '95 to
22 '96, maybe '97. I'm not sure. Somewhere in that range.

23 Q. Okay. And where did you go to work?

24 A. I went to a company called SAIC.

25 Q. All right. And that's the -- what's the full

1 name of that company?

2 A. Science Applications International
3 Corporation.

4 Q. And that's a company that Mr. Munger already
5 worked at by the time you joined it, correct?

6 A. Yes, sir.

7 Q. Did you meet Mr. Munger for the first time at
8 SAIC?

9 A. That's correct.

10 Q. Why did you decide to leave ARCO and go to
11 work at SAIC?

12 A. SAIC was really a very interesting company.
13 It was employee-owned. It was founded by a nuclear
14 physicist. Their management was all very technical and
15 just very good, very talented. It was an exciting place
16 to go, and I decided to go there.

17 Q. What did you begin doing? What kind of
18 projects did you begin working on at SAIC?

19 A. The first project was a secure satellite
20 communication system supporting the Global Hawk program.

21 Q. Now, we heard -- I guess you didn't hear
22 yesterday, because you weren't in the courtroom when Mr.
23 Munger testified. But the rest of us heard testimony
24 from Mr. Munger yesterday about the Global Hawk project.
25 Is that the unmanned aircraft that was used -- or at

1 least conceived, initially, to deal with scud missiles?

2 A. Yes, sir.

3 Q. What did Mr. Munger do on that Global Hawk
4 project?

5 A. Gif was the chief architect, which meant
6 that he -- he kind of -- he kind of worked on the --
7 whoops -- excuse me -- on the high-level concepts and
8 architecture of what the system ought to look like and
9 what the system ought to do.

10 Q. What did you do?

11 A. I -- I was system engineer and detail design
12 for this -- this secure satellite communication network
13 that we created.

14 Q. Now, you mentioned satellite communication.
15 We heard yesterday from Mr. Munger that the satellites
16 that the Global Hawk communicated with were not owned by
17 the military but were public or commercial satellites;
18 is that correct?

19 A. Yes, sir, that's correct.

20 Q. Was this unusual for a military project?

21 A. This -- this was definitely something that was
22 new at that time period, yes, sir.

23 Q. Did it create some particular challenges?

24 A. Yes, it did.

25 Q. What -- what were they?

1 A. Well, you know, prior to that time, military
2 used something called Mil SatCom, which they owned all
3 those assets. They secured all -- all those satellites.
4 So things were secured by the military.

5 When they started using the public or the
6 commercial satellites -- these are the same kind of
7 satellites that TV comes down on and that kind of
8 thing -- you had to worry about securing information
9 that was coming across the satellites, because anybody
10 could listen in on those, and if you didn't have some
11 mechanism of -- or some way of securing them, then the
12 bad guys could intercept your communications.

13 Q. And were you able to solve this challenge for
14 the Global Hawk project?

15 A. Yes, sir, we did.

16 Q. Was Global Hawk a successful project?

17 A. It was very successful.

18 Q. Is it used today?

19 A. Yes, it is, sir.

20 Q. And did members of your team at SAIC actually
21 play a role on the ground?

22 A. Yes, sir. There were members of my team --
23 this was back not long after 9/11, when they went into
24 Afghanistan, and then went into Iraq. We had members of
25 our team take our system out and set it up and operate

1 it to help the soldiers.

2 And they were able to get real-time pictures
3 of the battlefield and actually save -- saved lives with
4 it.

5 Q. Now, Dr. Short, was your experience with
6 Global Hawk important in leading to the inventions in
7 this case?

8 A. Yes, sir, it was.

9 Q. What was the next project you became involved
10 with at SAIC after Global Hawk?

11 A. This was a project that came to be known in
12 the early days as NetEraser.

13 Q. NetEraser?

14 A. Yes, sir.

15 Q. And what did Mr. Munger do? What was his role
16 on that project?

17 A. Well, he was our chief architect again,
18 serving a similar role as he did in the Global Hawk
19 where he was looking at kind of high-level concepts and
20 ideas and how to put the thing together and what it --
21 how it should work.

22 Q. Sounds like what you're trying to say,
23 Dr. Short, is that Mr. Munger would think of some ideas,
24 then you were stuck with making it work.

25 Is that about it?

1 A. Yes. We've had that relationship for
2 almost -- I don't know -- 20 years now maybe.

3 Q. And is that the role you played on the
4 NetEraser project?

5 A. Yes, sir.

6 Q. Who was the NetEraser project for?

7 A. This was done for a company called In-Q-Tel,
8 which was set up by Congress -- and I believe this was
9 in the opening statements -- to help the CIA identify
10 emerging technologies that -- to promote
11 commercialization of those technologies in a way that
12 would support the CIA's mission.

13 Q. And what in particular did the CIA need you to
14 help them do?

15 A. Well, they were looking for ways to provide
16 really secure communication between their -- their
17 agents and their operatives out in the field back
18 through to either the home office or regional offices,
19 and be able to do that across the internet in a way that
20 couldn't be detected or couldn't be intercepted.

21 Q. All right. Dr. Munger (sic), you -- you've
22 have just taken us up -- Dr. Short -- sorry.

23 A. That's all right.

24 Q. You've just taken us up to the NetEraser
25 project, and you've just described for us the need that

1 the CIA had to be able to compute and communicate safely
2 over the internet.

3 But right now, before we go on with that
4 story, I'd like you to help us understand better some of
5 the things that we've already heard about in the case
6 and some of the things that we're going to be hearing
7 about when we continue your story about how you came up
8 with that invention.

9 So tell us, please, what is the internet?

10 A. Well, I brought some pictures that will help
11 that.

12 Q. Okay.

13 A. This is kind of a simple example of how most
14 users interact on the internet or with the internet.
15 And most users, they've got a computer in their home at
16 their kitchen desk, table, or, you know, they have a
17 laptop that they're connected to the internet.

18 They may be in an internet cafe with a laptop
19 even, but they're sitting at their computer. And they
20 want to access information that's on the internet.
21 Maybe they're shopping on the internet; maybe they're
22 doing online banking. But they're trying to access
23 information and interact generally with another company,
24 companies on the internet, quite often.

25 So they're -- they're going through this cloud

1 here.

2 Q. Let me -- let me -- excuse me for interrupting
3 you.

4 A. Yes, sir.

5 Q. -- Dr. Short, but I want to make sure we
6 understand what we see on the screen.

7 The thing in the upper left that's labeled
8 remote user, what is that a picture of?

9 A. This is -- this is the user's computer.

10 Q. That's -- that's supposed to be a laptop
11 computer like several of them that we see around the
12 courtroom?

13 A. Can be a laptop, can be a desktop in the
14 kitchen.

15 Q. Okay. On the far right lower corner, what is
16 that gray box?

17 A. This down here is what's often referred to as
18 a server computer or a data server. It's generally
19 setting at some company. Like if you go in to shop at
20 JC Penney's, they'll have these data servers where
21 you're actually going and getting information.

22 Q. Okay. So the thing in the lower right is also
23 a computer but a different kind of computer?

24 A. Yes, sir.

25 Q. Does it have a screen usually?

1 A. Normally not.

2 Q. Okay. So -- so it doesn't -- it's not a
3 computer that people sit down and look at things on the
4 screen and type on a keyboard?

5 A. That's correct.

6 Q. And in the middle you've got something labeled
7 internet that looks like a cloud. Why have you drawn a
8 cloud there?

9 A. Well, people generally put a cloud there
10 because -- my hand is shaking; I'm sorry. I have
11 this -- I lost my mouse.

12 You have to pardon my hand shake. I have this
13 hereditary problem.

14 They -- generally, what really the internet is
15 all about is, there's a very large number of computers,
16 and they're interconnected with communication lines of
17 some form -- wires or fibers or something -- that really
18 make up the internet.

19 Q. Now, you've -- you've drawn a whole bunch of
20 little computers inside what we first saw as the cloud;
21 is that right?

22 A. Yes, sir.

23 Q. Is there a particular name for what most of
24 those computers are?

25 A. Well, these are -- these are routers, what are

1 called routers.

2 Q. Routers?

3 A. Yes.

4 Q. And what is a router?

5 A. A router is a special computer that is
6 designed to help to send information across the
7 internet. And what they do is a router has multiple
8 communication paths coming into it. And so information
9 will come in from one side, and the router will look at,
10 well, where's that supposed to go?

11 And based upon where it's ultimate destination
12 is, it will decide what's the best path to send it from
13 here? And then it will forward it along that path to
14 the next router.

15 And that router basically does the same thing
16 until, ultimately, it gets to its final destination.

17 Q. Now, I see that you've drawn the router
18 computers in your picture as having screens or monitors.

19 In fact, do routers usually have screens or
20 monitors?

21 A. Routers do not, no, sir.

22 Q. Why have you drawn these little computers with
23 screens?

24 A. Well, I put screens on them, because it makes
25 them look like computers. I mean, most of us think of

1 computers having a screen. And so it's just more
2 natural.

3 Q. Where -- where are these router computers
4 located?

5 A. These are located throughout the country. For
6 example, there will be a router in this courthouse
7 somewhere that these computers are connected to across a
8 radio link.

9 And then the router in this courthouse is then
10 connected through some -- some internet service provider
11 connection to a router at that provider, and then that
12 provider has a router connected to another router. And
13 so it just kind of spreads out.

14 Q. In fact, not only all over the country but all
15 over the world?

16 A. That's right.

17 Q. Who owns the internet?

18 A. Well, no single person or organization owns
19 the internet. It's -- it's owned by a very fairly large
20 number of organizations, people that -- that operate
21 collaboratively in a way where they interconnect with
22 each other.

23 And so you'll have -- you'll have information
24 being sent from one person -- or one organization's
25 router will go to another organization's router to

1 ultimately get it to the destination it's supposed to go
2 to.

3 Q. Now, Dr. Short, when someone wants to send a
4 message over the internet, how does the internet know
5 where that message is supposed to go?

6 A. They use something called a -- let's see if I
7 can get over here -- something called an IP address.

8 Q. What's that?

9 A. An IP address, as you see down here in the --
10 in the lower right, is a -- on the internet is a
11 four-digit sequence. It's unique to that computer's
12 location on the address. So every computer's public
13 ad -- excuse me; sorry -- public address on the internet
14 has a very unique sequence of four numbers.

15 Q. So every -- every computer hooked up to the
16 internet has its own number?

17 A. Yes, sir.

18 Q. Well, if -- if a user wants to use the
19 internet, though, to send a message to that computer,
20 how does the user keep track of all those numbers?

21 A. Well, fortunately, users don't have to. And
22 the people who -- who invented the internet were
23 actually, I think, had a lot of foresight and actually a
24 lot of insight about people. And they realized that
25 people aren't very good at remembering a lot of numbers.

1 I'm terrible at remembering numbers.

2 But people are good at remembering names and
3 words and particularly words that they associate.

4 For example, if you know you want to go to a
5 web page at Google, then it's easy for you to remember
6 Google.com, but you're not going to the remember their
7 numeric address.

8 Q. Is there a name for that -- that -- I guess
9 name -- is there a name for the name Google.com?

10 A. Yes, sir. Those -- those became known as
11 domain names.

12 Q. So Google.com is a domain name?

13 A. Yes.

14 Q. And Amazon.com is a domain name?

15 A. That's correct.

16 Q. And CNN.com is another domain name?

17 A. That's correct.

18 Q. Okay. How does that work then?

19 A. Well, the way that works -- to talk about
20 that, let's go and look at how this -- this actually
21 goes across the internet when I have this address, okay?
22 This address is being used to send this information that
23 we have depicted as -- as an envelope here, because it's
24 a lot like sending mail. You know, you put an address
25 on the mail -- on the envelope and you send it -- send

1 it across the internet.

2 And these routers are using that number to
3 decide how do I send it?

4 Q. So that's how the router uses that number,
5 right?

6 A. Yes, sir. That's right.

7 Q. But now tell us how the domain name helps
8 people send messages just like that without having to
9 remember the numbers.

10 A. So the way that works -- and I'm going to use
11 Google that I mentioned earlier as -- as an example.
12 Most people probably know what Google is, but for those
13 who might not, on the internet, one of the very useful
14 things you can do is -- is search for information.

15 There's all kinds of information on the
16 internet.

17 You can get recipes on the internet. You can
18 get how do I fix something on the internet. If you have
19 a -- if you have a broken appliance, you can go on the
20 internet and find out what the part is that you need.

21 You can shop on the internet. It's amazing
22 the amount of information on the internet.

23 The problem is that there's so much
24 information, how do you find it? And there's some very
25 popular search sites -- and Google is one of those --

1 that allows you to go to Google and you type in some key
2 words that you're searching for.

3 So if it's information about something, you
4 type in the things you want information about, and
5 Google will go out on the internet and come back and
6 say, here's a list of sources of -- of information that
7 you can go to, to read about this subject.

8 Q. Okay. So you've told us why someone might
9 want to find the Google page for their computer, but --
10 but tell us how that works.

11 A. Yes.

12 So the way that works is, if I want to go and
13 get this -- to the search page is, I use this domain
14 name, www.google.com. And so I go to my web browser,
15 okay, and I'm going to type in Google.com, but before I
16 do that, the inventors of the internet had to come up
17 with a system or a way to translate that Google.com into
18 the numeric address.

19 And what they came up with was this thing
20 called a domain name service.

21 Q. Have you drawn another box that is labeled
22 domain name service?

23 A. Yes, sir.

24 Q. What does the domain name service do?

25 A. What the domain name service does is think

1 of -- think of it as a big phone book, okay? So say --
2 say you want to get your car fixed and you want to call
3 Midas and get an appointment, but you don't know their
4 phone number.

5 You go to the phone book and you look up Midas
6 and across from Midas is the phone number.

7 Well the domain name service is very similar.
8 Is -- is you know you want to go to Google, but you
9 don't know how to get there, okay? So the -- the
10 internet system itself, including the user computer, can
11 use this domain name service and go to it to look up --
12 look up that name -- that name and find the
13 corresponding address.

14 So you type in Google.com. You hit return on
15 your browser, and your computer takes care of the rest.
16 It sends a request for a name look-up called a name
17 look-up to this domain name service, and that domain
18 name service looks up the name just like you would in
19 your phone book, except it's all done by computers. And
20 it finds the corresponding numerical address.

21 That numerical address is then sent back to
22 your computer. So now your computer knows what
23 numerical address to go to to get that -- that Google
24 page that you want, and to do that it builds what's
25 called a packet.

1 And a packet is like a chunk of data with
2 addressing on the front of it. And that's the way all
3 information on the internet sends using these packets.
4 The address that was just received from the domain name
5 service is put into the destination. That tells the
6 entire internet, when it sees that packet, where to --
7 where are we trying to send this -- this information to?
8 And then the source address over here is the -- that's
9 the address of the user's computer. And the reason
10 that's important is that tells Google where to send the
11 reply back to.

12 So that request goes across the internet to
13 the Google data server, and the Google data server looks
14 at the page request and says, oh, you want our search
15 page. It loads the search page into a packet, one more
16 packet, sends it back across the internet.

17 And in this case, the destination address is
18 your computer address, and the source is this data
19 server.

20 So it sends it back. The user computer then
21 takes that information and displays that picture.

22 Q. All right. Dr. Short, are these
23 communications that you've shown us that go across the
24 internet typically secure?

25 A. No, sir.

1 Q. Can you show us an example of how a normal
2 communication on the internet would not be secure?

3 A. Yes, sir.

4 So we'll continue with this. Now, you've
5 gotten your Google search page, and say you want to find
6 out about the Caldwell Zoo in Tyler. Maybe you want to
7 find out if they've got some event scheduled or what
8 their hours are or how to get there.

9 But you type in Caldwell Zoo into the search
10 engine or the browser page. Now the user computer
11 builds that -- that request into this -- in this packet
12 again and sends it over to Google. But now what happens
13 is there's a hacker somewhere in this network.

14 Now, remember, this network is this very large
15 number of computers, very large number of connections,
16 and they can't all be secure.

17 Q. Who might this hacker be?

18 A. Pardon?

19 Q. Who might this hacker be?

20 A. He could be -- he could be somebody in Russia.
21 He could be somebody in China. The amazing thing is you
22 have hackers now who do this for a living. They -- they
23 just -- they just scan the network trying to get
24 information that is useful to sell.

25 Q. Okay. If after the hacker eavesdrops on the

1 information, then what happens to this packet that the
2 user is trying to send to Google to find out about the
3 Caldwell Zoo?

4 A. So he gets -- he sees that packet. He sees
5 the request that you've made. But the packet --
6 typically, the packet just goes on its way. And there's
7 no indication to you; there's no indication to Google
8 that anybody has even seen that information.

9 Q. Okay. Dr. Short, but why do we care? In
10 other words, why do we care if someone knows in Russia
11 or China, or wherever they may be, that we looked up
12 information about the Caldwell Zoo?

13 A. Well, you probably don't care about that.

14 Q. Is there other kinds of information, though,
15 that we care about a lot?

16 A. Yes, sir. You know, like I mentioned,
17 there's -- there's credit card information; there's bank
18 account information; there's personal identification
19 information; there's, you know, your pictures, your
20 e-mail, all kinds of things across the internet that you
21 just wouldn't want bad people to get ahold of.

22 Q. Can you give us an information -- an example
23 of how a hacker might intercept confidential business
24 information?

25 A. Yes, sir.

1 In a business sense, you may have an
2 employee -- in this case, we'll use the business Acme.

3 Q. Is that a building that you've drawn over on
4 the right?

5 A. Yes, sir. This is an office building; maybe
6 it's their corporate headquarters.

7 And -- and it's got an internal network here
8 with, you know, people's desktops and laptops all
9 connected internally. Then it has a connection out to
10 the internet.

11 And -- and you may have employees that are out
12 on the road who are doing sales or doing, you know,
13 business on the road, and they want to securely be able
14 to send messages back. They want to be able to send
15 messages back to Acme.

16 So -- so in this case, say we have an employee
17 who's maybe sitting at the airport waiting for the
18 plane, who's been in a meeting and has learned that --
19 that their competition is doing things that requires
20 them to really cut their prices to, you know, possibly
21 win a contract or proposing them.

22 So he or she wants to send this back to the --
23 to the corporate office to give them a heads up that we
24 got to do something here. You would not want that
25 intercepted by somebody that could then provide that

1 information to their competitors.

2 So, again, we have this hacker who intercepts
3 that packet, is able to see what the confidential
4 information is. The packet goes on its way. There's no
5 indication that that message has been compromised in any
6 way. But, in fact, it has.

7 Q. All right. Thank you for those explanations,
8 Dr. Short.

9 Let's go back now to the story of your
10 invention, and I think that before you gave us those
11 explanations about the internet and the problem of
12 internet security, I think you were at the point where
13 you were working on what -- a project for the CIA, a
14 project that you called NetEraser, and that you were
15 trying to find a way to make internet communications
16 more secure.

17 Do you remember that?

18 A. Yes, sir.

19 Q. In the course of that project, did you and
20 your team research some of the security solutions that
21 were already available by, let's say, the late '90s when
22 you were doing your work?

23 A. Yes, I did.

24 Q. So were there already some ways to secure
25 information traveling across the internet?

1 A. Yes, sir.

2 Q. Well, for example, lots of people back then,
3 probably, were already buying books on the internet with
4 a credit card.

5 Could hackers see that information?

6 A. Typically not.

7 Q. What kind of technique was being used to keep
8 that kind of communication secure?

9 A. There were techniques referred to as
10 encryption.

11 Q. Encryption. Can you show us how encryption
12 works for protecting internet communications?

13 A. Encryption is -- we think of encryption as
14 scrambling information in a way that somebody who
15 doesn't know how it was scrambled doesn't know how to
16 unscramble it.

17 And in computers, the way this information is
18 scrambled is there's something called a secret key.

19 And -- and this secret encryption key is
20 combined with a set of methods to take this information
21 that you can read, and you apply the secret key with
22 these methods, and what comes out is this scrambled
23 data.

24 And then this scrambled data -- you see what's
25 happening here. The user computer has this encryption

1 capability. It is taking the information that's in this
2 data packet and is using the secret key to scramble
3 them.

4 Now, the only way to unscramble this
5 information is to know what the secret key is. The
6 methods themselves are known, but it's not good enough
7 to know the method. You have to know the secret key.

8 So this packet gets sent on its way. It gets
9 intercepted again by a hacker. Now, the only way the
10 hacker can decipher or understand what this message here
11 is, is they have to have the secret key to unscramble
12 it.

13 Since they don't have the secret key and the
14 only other computer that has the secret key is going to
15 be this data server from this computer right here at
16 Acme, that computer is the only one that's going to be
17 able to unscramble the message. So that's the way it's
18 protected.

19 Q. Are there any limitations on this internet
20 encryption technology that you just described?

21 A. Well, what I illustrated here was a -- a
22 point-to-point encryption.

23 Q. What do you mean by that?

24 A. Well, what I mean is that the encryption
25 started up here, and then it ended here (indicates), and

1 then that's where the message ended.

2 Q. So what -- what good is this point-to-point
3 encryption technology?

4 A. Well, it's very useful for a lot of -- a lot
5 of applications on the internet where you're going --
6 where you're using your web browser, and you -- you want
7 to do like online banking, or you want to do shopping
8 and you put in your credit card, because the information
9 only goes to this computer here. And this is the
10 computer that's -- that's handling the online banking
11 for you.

12 So as long as it's secure between those two
13 points, you're okay.

14 Q. Is there a name for this point-to-point
15 encryption technology?

16 A. The -- the most common version of this is
17 what's called https.

18 Q. What do the initials https stand for?

19 A. It's hypertext transfer protocol secure.

20 Q. Did you research this https point-to-point
21 security technology when you were looking for a solution
22 for the CIA?

23 A. Yes, sir.

24 Q. Was it good enough for what the CIA needed to
25 do?

1 A. No, sir, it was not.

2 Q. Why not?

3 A. Well, they wanted to allow their employees and
4 agents who were remote to have access into their private
5 network, to resources inside their private network.

6 Q. Could a point-to-point do that?

7 A. No, sir.

8 Q. So if this kind of security that was available
9 in the late '90s wasn't good enough for what the CIA
10 needed, was there another kind of technique for securing
11 internet communications that you were familiar with and
12 that you and your team considered in the late '90s?

13 A. Yes, sir.

14 Q. What was that?

15 A. That was a class of techniques called virtual
16 private networks.

17 Q. We've heard about virtual private networks
18 already, but even though Mr. Munger explained to us what
19 the words mean, can you explain to us now, how does a
20 virtual private network work?

21 A. Yes, sir. Go back to the Acme example. You
22 recall we have this Acme facility here, being the
23 corporate office, and inside it is a network with
24 computers on it.

25 And this network is referred to as a private

1 network. And the reason it's private is that it's
2 physically secured by the building itself and the locks
3 on the doors, so somebody outside the building doesn't
4 have access to information flowing through that private
5 network.

6 A virtual private network allows one to extend
7 the privacy on this private network across the public
8 internet to some computers remotely connected on the
9 internet.

10 Q. Okay. How does it work?

11 A. So one example of how it works -- we'll go
12 back to the message: Cut our prices. And you notice in
13 this example, we have some private addresses here
14 corresponding to this private network.

15 And in this case, the scrambling is occurring
16 not only on the information, but it's also scrambling
17 the addresses.

18 Q. So what happens then?

19 A. So this scrambled packet is put inside what
20 I'll call the public -- the public packet. And the
21 reason I call it the public packet is that it has the
22 public addresses used to route this across the internet.

23 So that's going to go on its way. Again, you
24 know, our bad guy is intercepting it, but you notice
25 this bad guy, all he sees is all the scrambled data

1 here. They're not even going to be able to tell that
2 it's a packet, frankly, because it's just garble to
3 them.

4 Q. Is the hacker able to see the address of the
5 recipient where the message is going?

6 A. No, sir.

7 Q. Is he able to see the content of the message?

8 A. No, sir.

9 Q. So what happens then with the message?

10 A. Well, that message arrives here at Acme. It
11 gets -- this private packet gets unscrambled. And so
12 now this computer here knows where to send the private
13 packet within that private network. So it sends it up
14 to the desk up here.

15 Q. Now, you -- you've shown us a simple message,
16 Cut our prices today, but what kinds of information or
17 data can be sent over these virtual private networks?

18 A. All right. You can really send any kind of
19 information. You know, any information that can be sent
20 over a network can be sent over a virtual private
21 network.

22 Q. And how is the virtual private network
23 different from the encryption technology you told us
24 about a few minutes ago?

25 A. Well, you notice in this case, the -- the

1 remote computer was able to send this message to a
2 computer within the private network; in other words, had
3 access to computers or resources within that extended
4 network.

5 Q. So when you and your team were doing this work
6 on behalf of the Central Intelligence Agency in the late
7 '90s, did virtual private networks already exist?

8 A. Yes, sir.

9 Q. And were you and your team already aware of
10 them?

11 A. Yes, sir.

12 Q. So did you then evaluate the products that
13 were available to set up VPNs as part of your project
14 for the CIA?

15 A. Yes, we did.

16 Q. And were there various kinds of software and
17 hardware that could be used to set up VPNs back then?

18 A. Yes, sir.

19 Q. Did you and your team buy them and study them?

20 A. We did. We looked at -- we looked at a number
21 of different products that implemented what was becoming
22 the industry -- appeared to becoming the industry
23 standard in virtual private networks using IP SEC.

24 Q. Were they practical solutions?

25 A. Once you had them set up, they worked. They

1 were -- they were -- they were difficult to set up and
2 pretty complex, which for the average user, they
3 certainly were not practical.

4 Q. Did you -- in fact, you and your team of
5 experts sometimes have problems setting them up?

6 A. It was not unusual for us to go through a
7 setup procedure and have it not work and then have to
8 debug or figure out what mistake that we made and go
9 back and fix it and do a couple of iterations to get it
10 to work.

11 Q. So, Dr. Short, can you -- instead of just
12 telling us that, can you actually show us an example of
13 the kind of things that would have to be done to set up
14 a VPN in this timeframe?

15 A. Yes, sir.

16 Q. Let me show you Plaintiff's Exhibit 983. What
17 is this document?

18 A. Let me put my glasses on.

19 This is the -- it's a -- it's a how-to help
20 document provided by Microsoft support to help users
21 with the steps that one goes through to set up a -- an
22 IP SEC tunnel, which is a VPN, in the Windows 2000
23 operating system.

24 Q. Have you blown up the pages of this exhibit
25 large so that you can walk the jury through what was

1 required?

2 A. Yes, sir.

3 MR. CAWLEY: Your Honor, may I request
4 that the witness step down to an easel over here?

5 THE COURT: All right.

6 Q. (By Mr. Cawley) Now, Dr. Short, this is the
7 first page of Plaintiff's Exhibit 983?

8 A. Yes, sir.

9 Q. I notice that there are a number of dates on
10 it. Can you tell us about those dates?

11 A. Well, there's a date down here in the corner
12 (indicates), January 27th, 2010. That's the date this
13 was -- was printed out.

14 There's a couple of dates up here (indicates),
15 July 13th, 2010, which it's -- Microsoft's office is
16 notifying users that this is when they end their
17 official support on the Windows 2000 operating system.

18 Q. What does this document tell us how to do?

19 A. This document is going to take a user through
20 the steps of the things, the steps you go through to set
21 up a virtual private network in the Windows 2000.

22 Q. Now, when was the Windows 2000 software
23 available?

24 A. That came out in 2000.

25 Q. Okay. And did you -- is this a document from

1 Microsoft?

2 A. Yes, sir.

3 Q. It's available on the internet to tell anybody
4 who wants to know how to set up a VPN using the software
5 available back in 2000; is that right?

6 A. Yes, sir.

7 Q. Okay. And did you use documents and software
8 similar to this to set up VPNs when you were evaluating
9 security on the internet for the CIA?

10 A. Yes, sir, we did.

11 Q. Actually set up VPNs similar to the way you're
12 about to show us?

13 A. Yes, sir.

14 Q. All right. So, Dr. Short, using this
15 document, basically, as an instruction manual, take us
16 through the steps that would have been required, say,
17 back in 2000 if somebody wanted to use Windows 2000 to
18 set up a VPN.

19 A. Okay. So this -- the instructions, in terms
20 of the steps, start here on Page 2 of the document,
21 begins with creating an IP SEC policy.

22 Q. Okay. What would you have to do to get that
23 accomplished?

24 A. There's -- there's five steps here that are
25 outlined for creating this policy.

1 The first one is -- is you have to run
2 something called MMC. And once you start the MMC, you
3 have to load something called the IP security snap-in.
4 And then having loaded that snap-in, you click start and
5 run and then type in this secpol.msc. And so that's the
6 first step.

7 The second step here is right click on the
8 security policies for your local machine, and then
9 you're going to click and say I want to create an IP
10 security policy. So that's the second step.

11 The third step, clicking next, asks you to
12 type in a -- a name here -- I can do it this way -- a
13 name for your security policy, so you can refer to it in
14 the future.

15 And then you go on to the fourth step. You
16 want to clear this activate default response rules
17 because you're going to do some manual -- enter in some
18 manual rules. Click next.

19 And then finally the fifth step is click
20 finish.

21 Q. Okay. So you've done those five steps. Do we
22 have a VPN?

23 A. No, sir.

24 Q. What's the next thing we've got to do?

25 A. Okay. Now we're going to start actually

1 defining what's in the VPN as in how does it behave.

2 And the first step there is -- it's this thing called
3 the filter list --

4 Q. Okay. And how many things do you --

5 A. -- from Net A to Net B.

6 Q. I'm sorry. How many things do you have to do
7 to set this up?

8 A. Well, there's nine steps here.

9 The first step, you're wanting to use this
10 wizard, and once you get in the wizard, you're going to
11 add to create a new rule.

12 After that step, you're going to go to the IP
13 filter list tab, and you say, I want to add an IP filter
14 list.

15 And then you go to the third step. You're
16 going to clear -- in this case, you're going to clear
17 the use add wizard check box, because you're going to do
18 things manually, and then click add.

19 And then on the fourth step -- this is where
20 it gets kind of interesting because you have to start
21 defining your -- your private address locks on each
22 side. And there's -- there's a source address on one --
23 on one side; there's a destination address for the other
24 side.

25 And so the first thing is you're going to find

1 this source address. And the source address is -- what
2 you're doing is specifying a specific IP subnet.

3 You remember those IP numbers I told you
4 about, those four numbers? Well, you have to identify
5 one of those four numbers of that set of four numbers
6 called the IP address, and then there's something called
7 subnet mask, which is -- that's -- that's a network
8 engineering term that limits what you can put on that
9 network.

10 You go to step five, and now you have to do
11 the same thing on the destination side. You're going to
12 specify the subnet here, which includes, again, another
13 IP address, and then another subnet mask.

14 This is where -- this is partly where I say
15 the average user is going to become overwhelmed, I mean,
16 because unless you're a network engineer, you don't even
17 know what this stuff means. And so you really need a
18 network engineer to help you through this process.

19 You go on to step six, and you clear the
20 mirrored check box, and then you specify something
21 called protocols, which, basically, is what kind of
22 communication will you allow over this VPN. And you say
23 I don't allow any kind.

24 And then in step eight, you're going to --
25 you're going to click the description and type in a

1 description, and then finally, here you click okay and
2 close out.

3 Q. Okay. With all those steps you've taken us
4 through, do we have a VPN yet?

5 A. No. No, sir.

6 Q. What's the next thing we've got to do?

7 A. We now have to do the same thing pretty much
8 to go from Net B to Net A because I got two sides to my
9 VPN.

10 Q. Show us the steps for that. How many steps
11 are there to do that?

12 A. Well, we have seven steps -- excuse me --
13 seven steps up here.

14 Q. Okay. Let me -- let me interrupt you.

15 Judge Davis told us just a little while ago
16 that we all have limited time, so let's just cheat.
17 Check off those steps, but don't tell us anything about
18 it.

19 A. Okay. So there's seven steps.

20 Q. Okay. Do we have a VPN now?

21 A. No, sir.

22 Q. What have we got to do next?

23 A. Now I have to specify these -- these rules
24 between Net A and Net B.

25 Q. How many steps to do that?

1 A. There's ten of those.

2 Q. Check all those off.

3 A. (Complies.)

4 Q. Now, what do we have to do next?

5 A. Now I have to go from Net B back to Net A and
6 specify a rule for that. And I have seven steps on
7 that.

8 Q. Now, do we finally have a VPN, Dr. Short?

9 A. Well, I've entered in all my parameters pretty
10 much for my VPN, but because there's so much information
11 being put in here and it's critical that that
12 information is self-consistent, that is that it doesn't
13 conflict with itself, that they recommend that you
14 really kind of print it out and check it to be sure
15 you've got everything the way you think you should have
16 it.

17 Q. Can you show us that?

18 A. So this -- this is an example of what this
19 printout would be here, and there would be a lot of
20 values in here instead of these zeros. But this is the
21 summary of all the configuration choices you made and
22 all the parameters that you -- values that you entered
23 in.

24 Now, the thing to keep in mind is that on a
25 VPN, you have two sides. And so we've configured one

1 side.

2 Now, I've got another user -- nor network
3 engineer really -- at the other side, who is doing the
4 same thing.

5 Q. They've got to go through all these steps on
6 the other end?

7 A. Yes, sir.

8 Q. And, in fact, this is a network, right?

9 A. Yes, sir.

10 Q. So it's not just two ends usually, correct?

11 A. If you're adding another -- another computer
12 to the VPN, then you're going to go through this process
13 again, yes, sir.

14 Q. How long did this take?

15 A. Including the time -- I mean, typically, the
16 way this would work is a -- network engineers would be
17 asked to set up VPNs.

18 And they would get on the phone with each
19 other, and they would -- they would negotiate what this
20 configured -- configuration should look like, because
21 these values have to work within their -- their current
22 network.

23 And so they would negotiate what those values
24 ought to be, and then each would go and do their
25 configuration.

1 Q. And how long would it take?

2 A. And so you're talking 30 minutes to an hour
3 from the time that they've gone through and talked it
4 out, they've put in the configuration, and then they
5 check it out. And if it works the first time, they're
6 really lucky, I think, or they've done it a lot of
7 times.

8 Q. Okay. Well, once this is set up, does
9 Microsoft then recommend that it be tested?

10 A. Yes, sir.

11 Q. And how would it be tested?

12 A. Let's see. I don't think that's it.
13 Okay. Testing -- it talks about here testing your IP
14 SEC tunnel, which, again, to remind you, this is our
15 VPN -- they -- they have this tool called the IP
16 security monitor. And they recommend you run this IP
17 security monitor to see the activity going on in the
18 virtual private network to make sure it's working.

19 And to do that, they recommend using something
20 called a ping command, which is basically a request for
21 an echo reply. It's where one computer sends an echo
22 request to the other computer. The other computer gets
23 that echo request and sends a reply back.

24 Q. Okay.

25 A. So that tells you you have a connection.

1 Q. Okay. Dr. Short, I think we'll come back to
2 that echo test in a few minutes, but what if the test
3 doesn't work?

4 A. Well, if the test doesn't work, then you need
5 to go back to what did my configuration look like, and
6 what could possibly be wrong?

7 And there's a good chance you're going to get
8 on the phone with the network engineer on the other
9 side, and they're going to talk it out and say, well,
10 I'm not seeing any packets, or they're not encrypted, or
11 what's the problem here and kind of go through and see
12 if you can identify where the problem is.

13 Q. Okay. Dr. Short, I think we're through with
14 that document. If you would return to the witness
15 stand, please.

16 A. (Complies.)

17 Q. Now, Dr. Short, you've just shown us, using
18 Microsoft's own instruction manual, how someone would
19 have set up a VPN using Microsoft software in the year
20 2000.

21 Did you and your team examine products similar
22 to this?

23 A. Yes, sir, we did.

24 Q. And did they have similar issues of being
25 complicated and hard to do?

1 A. Yes. They were all very similar, in terms of
2 the kind of parameters, the kind of choices you had to
3 make. Some of them you had to put all this
4 information -- type it into a text file. Some of them
5 you had to type in commands to the device.

6 But they were all very similar in terms of the
7 same kinds of parameters, the same kinds of choices, and
8 the same kind of knowledge that you had to have to do
9 that.

10 Q. So, Dr. Short, did this provide security in a
11 practical sense?

12 A. You know, like I said earlier, I don't think
13 so, because, I mean, it was difficult for me, and I'm
14 not sure I ever got it right the first time. But for
15 someone who doesn't have any network knowledge, I don't
16 know how you would do it.

17 Q. How long did your team work on this problem
18 until you had a break-through?

19 A. We -- we worked on this probably for three to
20 six months. We had this vision of we're never going to
21 bring this kind of security to the average user if we
22 can't solve this problem.

23 Q. And did you finally have a break-through that
24 at least was the beginning of your ability to solve this
25 problem and the beginning of the invention in this case?

1 A. Yes, sir.

2 Q. Can you tell us about that?

3 A. Yes. We were -- we had gone up to New York
4 City for a meeting, and we were on a train coming back,
5 coming through New Jersey, and we had been thinking
6 about this problem, and I realized, actually, there were
7 two aspects to this problem.

8 One was that users type in -- or users
9 initiate -- try to get on the internet and connect to
10 things, but also applications do that without the user
11 doing anything.

12 So we -- we really needed to figure out, how
13 do we make VPNs so they just happen for people and they
14 just happen for applications?

15 And we were -- we were talking about, you know
16 how telephones work and that with telephones, people
17 just dial the number.

18 And in the old days, you had the old rotary
19 dial systems, and then they went to the touch tone, but
20 they didn't change the way people made phone calls; they
21 just changed from a rotary dial to a touch tone.

22 But all the changes were hidden from the user,
23 so it was just very natural for the user, that they were
24 getting a new way of doing connections.

25 So the thought was that somehow we've got to

1 figure out how to do this on the internet. And I
2 started thinking about, well, how do connections occur
3 on the internet? And I thought, well, people type in a
4 domain name, okay? That's how people start a
5 connection.

6 And then I said, well, how do applications
7 start a connection? Well, they have a domain name that
8 they do something called a get host by name, which it
9 says give me the numerical address.

10 So I said, oh, it's the same thing, because
11 when a user types in a domain name, hits return, the
12 computer says, what's the address?

13 When an application says, I need a connection
14 to a domain name, the computer says, I need an address.
15 So I thought, oh, they're both connecting the same way.
16 So the way we initiate VPNs is, we have to somehow
17 trigger on the fact that this computer is trying to get
18 a translation of this domain name to the corresponding
19 computer address.

20 Q. And how did you feel when you had that idea on
21 the train?

22 A. Oh, I was really excited.

23 Q. Did you tell Mr. Munger and Mr. Larson about
24 it?

25 A. Yes, sir.

1 Q. What was their reaction?

2 A. They were excited, too.

3 Q. Did you still have work to do, though, on
4 working out the details of your invention?

5 A. Yes, sir.

6 Q. And how much longer did your team work on the
7 invention?

8 A. I would say for this -- for this initial
9 concept, it was in September. By the end of the year,
10 we kind of had all the pieces that we knew we had to
11 bring together to -- to do this.

12 Because what we had to do was, all those
13 things that you saw there were things you had to do, and
14 you had to do them safely. Because if somebody was able
15 to see what you were doing, then your VPN wasn't going
16 to be secure.

17 So we had to figure out how to take all that
18 and do it safely.

19 Q. Can you show us how you did that? What --
20 tell us how your invention works.

21 A. Yes, sir.

22 Q. I think you can tap the screen to get rid of
23 that red arrow.

24 A. Hit clear?

25 Q. Clear last --

1 A. Oh, there it is.

2 Q. There you go.

3 A. Got it.

4 Okay. So the -- the first solution we came up
5 with, which I'll talk about first, is what's often
6 referred to as the '135 in this case.

7 Q. That's the '135 patent?

8 A. Yes, sir.

9 Q. Okay.

10 A. And in this case -- I'll refresh your memory.
11 You remember, the way the normal DNS works, the user
12 types in this name, the computer requests an address
13 from the -- from this domain name service, gets an
14 address back, and then uses that address, okay?

15 So what we had to do is, we had to get in the
16 middle of that, because we wanted to trigger a VPN.
17 Instead of just letting this thing go to the domain name
18 service and come back with some unprotected address, we
19 wanted to get in the middle of that.

20 So what we did was we created something called
21 a DNS proxy.

22 Q. What's that?

23 A. A DNS proxy is -- it's -- it's a software
24 module. Sometimes it's a computer. A lot of times it's
25 just a software module, part of a computer, that is used

1 to process a domain name request before it gets to the
2 domain name service.

3 So we said, ah, that's how we get in the
4 middle of this.

5 So in this case, what happens is, the user has
6 typed in the name. Now, instead of going to the domain
7 name service, it goes to the proxy. The proxy looks at
8 this and -- name and makes a determination.

9 The determination is, does this name
10 correspond to a computer where I can set up and have a
11 VPN? Can I have a secure connection with this -- with
12 this computer?

13 Okay. If the answer is no, it's not one of
14 those kinds of -- you know, it's not -- it's not that
15 location. That computer can't do that.

16 Then it forwards that request on to the
17 existing domain name service, which does its normal
18 lookup and returns the public address for that.

19 If the answer is yes, that this name supports
20 a secure connection, a VPN, then it builds something
21 that we call a VPN request, which, basically, is, hey, I
22 want a VPN with you.

23 Now, we needed something to handle that VPN
24 request. So to handle that VPN request, we created
25 something called a gatekeeper. And the gatekeeper, a

1 piece of software, can be a separate computer, doesn't
2 have to be, just a piece of software that receives that
3 VPN request. So that request goes over to the
4 gatekeeper.

5 Now, the job of the gatekeeper is to take that
6 request and build a VPN between the user's computer and
7 this requested target here.

8 Q. So is the invention that you just showed us
9 and described for us shown in your patent?

10 A. Yes, sir, it is.

11 Q. Let's -- let's take a look at Figure 26 of the
12 '135 patent.

13 Is that the invention that you showed us?

14 A. Yes, sir.

15 Q. Can you -- can you point out some parts of it?

16 A. For example, you see the DNS here, proxy. You
17 see the gatekeeper right here. I'm not very good at
18 drawing here. And you see how the request for this --
19 this name lookup goes to the DNS proxy first before it
20 goes to the DNS server.

21 And then -- so if it can support a VPN, the
22 request goes down here to the gatekeeper, and the
23 gatekeeper sets up this VPN, and you've got your VPN.

24 Q. All right. So, Dr. Short, you've just
25 described to us your invention in the '135 patent, and

1 you've told us a lot of things that happened to set up a
2 VPN, but remind us, in your invention, what does the
3 user, the human being sitting at a computer, who wants
4 to set up a secure connection, what do they have to do?

5 A. The user types in the domain name, just like
6 before and hits return.

7 Q. Hits one key?

8 A. Yes, sir.

9 Q. And then your invention does the rest?

10 A. Yes, sir.

11 Q. Now, can you tell us about the second patent
12 that you got, the '180 patent? How does that work?

13 A. Yes, sir.

14 The '180 patent is a -- is a second approach
15 method that we came up later with, which uses something
16 we call a secure domain name.

17 And so in this example, we've got -- this
18 remote user actually wants to send something over to
19 john.acme.scom. So in this example -- I'm sorry. I'm
20 pointing here, and you can't see where I'm pointing. Up
21 here (indicates).

22 And then this example is John sitting over
23 here at this desktop here, and his computer has a secure
24 domain name address, what we call it.

25 So the user types that in, hits return. Now,

1 normally what would happen is, this request would go to
2 your normal domain name service.

3 Now, john.acme.scom is not in that -- is not
4 in that directory, so it doesn't know where it is. It
5 sends a reply back, says, I can't find this name, okay?
6 So using our secure domain names, we had to come up with
7 something we call a secure domain name service, okay?

8 So this is a service that knows how to handle
9 secure domain names.

10 It can be just -- you know, like those other
11 two examples with the proxy And gatekeeper, it can be a
12 software module running on some computer, as long as you
13 have access to it -- it doesn't matter where it is -- or
14 it can be a standalone computer, either way.

15 Q. So what happens then?

16 A. So at that point, we have now the -- the user,
17 again, types in this secure domain name, this .scom
18 name, and it goes over to the secure domain name
19 service.

20 Now, the secure domain name service, okay,
21 looks at that to see if there's a corresponding secure
22 address.

23 Q. What does that lock represent?

24 A. That lock represents, one, that the address is
25 a secure address and that it can also provide

1 provisioning information back to the user's computer.

2 Q. And what's that?

3 A. And what I mean by provisioning information
4 is -- you know, all those parameters I was doing over
5 there where I was specifying addresses and -- and
6 ultimately you have to specify keys and things like
7 that, well, that's called provisioning information for a
8 VPN.

9 And so some of that information could actually
10 be provided by our secure domain name service back to
11 the user's computer.

12 Q. All right. After the request goes to the
13 secure domain name service, what does it do?

14 A. Okay. So that comes back to the user's
15 computer, and then the user's computer can use that
16 address and send an access request message across the
17 VPN up to its destination, to John.

18 Q. Now, does this '180 patent require a
19 gatekeeper?

20 A. No, sir.

21 Q. Now, Dr. Short, you've shown us a lot of
22 pictures, and you've told us a lot about how your
23 invention works and how it can set up a VPN.

24 Have you actually brought computers to the
25 courtroom today, and can you actually show the jury what

1 is required here in the courtroom live to set up a
2 virtual private network?

3 A. Yes, sir.

4 MR. CAWLEY: Your Honor, may the witness
5 step down to this computer?

6 THE COURT: Yes, he may.

7 How much longer do you have on direct?

8 MR. CAWLEY: Fifteen minutes.

9 THE COURT: Well, let's go ahead and take
10 a break, and we'll do that when we come back. We've
11 been going for about an hour and a half.

12 Ladies of the Jury, we'll be in recess
13 for about 20 minutes, until a quarter until 11:00. So
14 enjoy your break, and remember my instructions. We'll
15 be in recess.

16 COURT SECURITY OFFICER: All rise.

17 (Jury out.)

18 (Recess.)

19 COURT SECURITY OFFICER: All rise.

20 (Jury in.)

21 THE COURT: Please be seated.

22 All right. You may proceed, Mr. Cawley.

23 MR. CAWLEY: Thank you, Your Honor.

24 Q. (By Mr. Cawley) Dr. Short, I'm sorry. I think
25 I had just asked you if -- if you could demonstrate to

1 us, live in Court, how your invention would set up a
2 VPN. And I asked Judge Davis if you could step down to
3 your computer over here, and I think he said you could.

4 A. Thank you.

5 Q. So would you turn on your computer and tell us
6 when you're ready to go?

7 A. (Complies.)

8 Yes, sir.

9 Q. Okay. So let's first get clear what we see in
10 the courtroom.

11 Is this your computer that you're standing
12 next to?

13 A. Yes, it is.

14 Q. Is it hooked up to the internet?

15 A. Yes, sir.

16 Q. I see some wires coming out of it. One of
17 those is a wire for electricity, right?

18 A. Yes, sir. It's a power cable.

19 Q. And there's also a wire that has connected
20 your laptop to the projector so that the jury, when we
21 get there, will be able to see on the big screen what's
22 on your little screen.

23 A. Yes, sir. That's over here.

24 Q. All right. How is your computer connected to
25 the internet?

1 A. There's a -- what's called a wireless device
2 or a radio device that communicates over radio waves
3 with what's called a wireless router in the courthouse.

4 Q. So Judge Davis and the other people in the
5 courthouse make available a wireless connection to the
6 internet; is that right?

7 A. Yes, sir.

8 Q. And is there anything special about this
9 connection?

10 A. No, sir.

11 Q. So anybody who has a laptop computer like
12 yours and many others in the courtroom that have the
13 ability to connect wirelessly over radio waves can come
14 in, and if Judge Davis gives them the password, connect
15 to the internet that way, correct?

16 A. That's correct.

17 Q. All right. Is your computer connected to a
18 virtual private network?

19 A. No, sir.

20 Q. Okay. Now, I also see that there's a computer
21 in front of Mr. Munger.

22 A. Yes, sir.

23 Q. Is Mr. Munger's computer connected to the
24 internet?

25 A. Yes, sir.

1 Q. How is Mr. Munger's computer connected to the
2 internet?

3 A. He has a wireless card that is connected to a
4 wire -- a little wireless cell card.

5 Q. What -- what does that mean?

6 A. Well, Verizon -- show it there -- Verizon
7 makes this little cell card, which is actually like a
8 little telephone, and you send data across it, and it's
9 actually got a little wireless device in it where
10 laptops can hook into that and then get to the internet.

11 Q. So Mr. Munger's computer is also connected to
12 the internet wirelessly; is that right?

13 A. Yes, sir.

14 Q. But it's connected in a different way than
15 your computer is?

16 A. Yes, it is.

17 Q. So is it fair to say that your computer is
18 connected to one part of the internet and Mr. Munger's
19 computer is connected to another part of the internet?

20 A. Yes, sir. It comes into the internet from two
21 different locations.

22 Q. Now, let's get back to your computer.

23 What kind of software do you have running on
24 your computer?

25 A. We have our -- what we call our Gabriel

1 connection software.

2 Q. What is the Gabriel connection software?

3 A. This is a development we've been doing for the
4 last two and a half years. It's in beta right now, beta
5 testing. We have users test it and give us feedback on
6 it.

7 And it's running here in this window.

8 Q. Okay. So this -- this software that's running
9 on your computer is called your Gabriel software,
10 correct?

11 A. Yes, sir.

12 Q. You say that you and the other people at
13 VirnetX have been working on it for how long?

14 A. Something like two and a half years, I think.

15 Q. Is it finished?

16 A. No, sir.

17 Q. Is it in a test stage?

18 A. Yes, sir.

19 Q. And what's that testing called?

20 A. We call it a beta test.

21 Q. Does this Gabriel software use your invention?

22 A. Yes, sir.

23 Q. Is there also Gabriel software on Mr. Munger's
24 computer?

25 A. Yes, sir. He has a very similar window like

1 here.

2 Q. And does this software use the invention that
3 you told us about just about 20 minutes ago that is in
4 your patents that can be used to set up a virtual
5 private network?

6 A. Yes, sir.

7 Q. Now, on the screen up here, we see what's
8 actually the same as this screen of your computer; is
9 that right?

10 A. Yes, sir.

11 Q. Okay. What's this big white rectangle or box
12 that we see on the screen of your computer?

13 A. This is -- this is the Gabriel application
14 window, what we call the client.

15 Q. Okay. And at the very top, is that window
16 labeled?

17 A. Yes, sir.

18 Q. What does it say?

19 A. It says VirnetX Gabriel Connection.

20 Q. What do we see in the white part of the box?

21 A. Down here, we see two computers that -- that
22 we can have connections with, secure connections.

23 Q. What's the first one called?

24 A. The first one you can see is called Gif.

25 Q. Can you use that arrow so we can see it?

1 A. You see that?

2 Q. Where is that computer?

3 A. That's -- that's Gif's laptop over there.

4 Q. Okay. And the second -- what's the name of
5 the second computer?

6 A. The second, you see there, is www.acme.scom.

7 Q. Where's that computer?

8 A. That's -- that's a computer in Virginia at a
9 data center.

10 Q. All right. Since Mr. Munger has a computer in
11 the room, let's connect to him by a virtual private
12 network. And first, let me ask you, before you do
13 that -- take that down.

14 Can you show us -- how will we know if your
15 invention is successful in establishing a virtual
16 private network over the internet back to Mr. Munger's
17 computer? How will we know that?

18 A. We have a little icon here that looks like a
19 little clock next to Gif's computer. And if we have a
20 secure -- he just -- he just moved his keyboard or his
21 mouse, which told us that he's now active on his
22 computer, so it changed the icon.

23 Q. Okay. So we see a little green --

24 A. Yes.

25 Q. -- bubble there?

1 A. And so when -- when we get a secure
2 connection, a VPN, that icon is going to change, and
3 there's going to be a little gold lock on the top of
4 that icon, which means that it's secure.

5 Q. That little icon, that green bubble?

6 A. Yes, sir.

7 Q. Is it pretty small?

8 A. For us old people, it's small, yes, sir.

9 Q. And let me ask Mr. Munger to step away from
10 his computer, because I want to see -- not step away,
11 but I want to see not anything Mr. Munger is doing. I
12 want to see what's working from your computer.

13 Using your computer hooked up to the internet
14 and using your invention on your computer, can you show
15 the jury what the user has to do to actually set up a
16 virtual private network?

17 A. Okay. So I've selected connect. It says the
18 word connection. And if I just hit the mouse button,
19 which is the mouse button, that's going to start the
20 connect process.

21 So this is negotiating a connection. And
22 we'll see a gold lock show up --

23 Q. Is that it?

24 A. -- right there (indicates).

25 A. Yes, sir.

1 Q. By pushing that one button and using your
2 invention, Dr. Short, did you succeed in setting up a
3 virtual private network with Mr. Munger's computer?

4 A. Yes, sir.

5 Q. And is that the same kind of virtual private
6 network that used to take network engineers going
7 through all the steps that you showed the jury about 45
8 minutes ago?

9 A. Yes, it is.

10 Q. And you did that with one click?

11 A. Yes, sir.

12 Q. And would it be just as easy to set up a
13 virtual private network with a computer in Virginia?

14 A. Yes, sir.

15 Q. Now, let's -- let's not go there, though.
16 Let's stay with Mr. Munger's computer.

17 Do you remember that ping test that you told
18 us about, that Microsoft suggested could be used to test
19 the connection over the virtual private network?

20 A. Yes, sir.

21 Q. Can you do a ping or echo test over the
22 virtual private network that you set up between your
23 computer and Mr. Munger's computer?

24 A. Yes, sir. I just opened up a little
25 application here that's the ping application. And so I

1 need to put this down so I can type.

2 So I typed in Gif's secure domain name, and we
3 hit return, and it starts sending the ping request,
4 okay? These are -- like I said before, these are the
5 little echo requests going to Gif's computer; his
6 computer sending a reply back.

7 And when a reply comes back, it prints out
8 echo received. So it sent five ping requests.

9 Q. So just in that amount of time you just showed
10 us, five times your computer sent a ping over the
11 internet out somewhere in the world and back down to the
12 courthouse to Mr. Munger's computer, which echoed it
13 back around the internet to your computer?

14 A. Yes, sir.

15 Q. And what else do we see in this box?

16 A. We see -- remember, we talked about these
17 private addresses that got scrambled. That's an example
18 of one there, that 172.19.13.135. That's a private
19 address that Gif's computer is using. And the little
20 lock there says this is a secure VPN.

21 So that address can get scrambled before it
22 goes out to VPN.

23 Q. Are you able to send messages securely back
24 and forth to Mr. Munger using this virtual private
25 network connection?

1 A. Yes, sir.

2 Q. Can you show us that?

3 A. Let me close this window.

4 We have a little chat application here we
5 built that allows me to type in a message. It will send
6 it to his computer.

7 Q. So you're typing a message at the very bottom?

8 A. Yeah.

9 Q. Looks like it says, hi, Gif, but you
10 misspelled it.

11 So have you sent that message securely to
12 Mr. Munger?

13 A. Yes, sir.

14 MR. CAWLEY: Mr. Munger, may I ask you to
15 reply to it from your computer?

16 MR. MUNGER: Yes, sir.

17 Q. (By Mr. Cawley) Is that the answer that
18 Mr. Munger just sent back through his wireless
19 connection over the secure virtual private network in
20 the internet over to your computer?

21 A. Yes. You notice it says Acme.com. This chat
22 application is using the same VPN channel.

23 Q. All right. Thank you, Dr. Short.

24 Would you take the witness stand again,
25 please?

1 A. (Complies.)

2 Q. Now, Dr. Short, you just told us or showed us
3 a chat that was going back and forth over the virtual
4 private network created by your invention between you
5 and Mr. Munger.

6 Is your computer, as it's currently set up,
7 accessing a website?

8 A. No, sir.

9 Q. Why not?

10 A. The -- we have -- we have something we call
11 security policy for our VPNs, which allows you to
12 control what the computer can access.

13 And Gif's laptop is not running a web server,
14 and the www.acme.scom, that one has a security policy
15 that's blocking any kind of access to a web server from
16 that computer.

17 Q. What would you need to do to access a website?

18 A. All you would have to do on the Acme computer
19 is change the policy for that laptop to say, allow the
20 web service through.

21 Q. How long would it take to do that?

22 A. Five seconds.

23 Q. Five seconds.

24 And once you make that change in policy, is
25 that persistent? In other words, does it stay that way

1 until somebody changes it again?

2 A. Yes, sir.

3 Q. Now, let's go back to the project -- your
4 NetEraser project that you were doing with Mr. Munger at
5 SAIC.

6 When did you deliver the NetEraser software to
7 the CIA?

8 A. We delivered source code, I'm guessing,
9 February/March timeframe of 2001.

10 Q. And did the CIA use the software?

11 A. I don't know.

12 Q. Why do you say that you don't know?

13 A. Well, the CIA is very protective about its
14 methods and particularly communication methods.

15 So if -- if -- they didn't need us. They
16 could take our software and do what they wanted to with
17 it. Likely, they wouldn't tell us.

18 Q. All right. Yesterday, we heard quite a bit of
19 testimony from Mr. Munger about trying to raise money
20 for your invention, talking to venture capitalists,
21 talking to various companies.

22 Did you participate actively in the effort to
23 find investors for your invention?

24 A. No, sir. I was not actively involved in that
25 side.

1 Q. Did you continue back at the shop to develop
2 the software for the invention?

3 A. Yes, sir.

4 Q. Did your employer, SAIC, though, agree to
5 invest money in that effort?

6 A. Yes, they did.

7 Q. Tell us about that.

8 A. We had -- we had a meeting briefing to our
9 CEO, Dr. Bob Beyster, in -- I believe it was January
10 2001. And we knew that the -- the -- the In-Q-Tel
11 contract was phasing down, and we were looking for SAIC
12 to invest to further the development of our prototype
13 and to try to help commercialize these ideas.

14 Q. So how much money did they invest?

15 A. As a result of that meeting, Dr. Beyster
16 approved 1.7 million, which was used to keep us going.

17 Q. Okay. And this is during the time that
18 Mr. Munger was out on the road trying to find additional
19 investment money, correct?

20 A. Yes, sir.

21 Q. But when Mr. Munger and others were
22 unsuccessful in raising that money, did SAIC eventually
23 decide that it would discontinue investing money and
24 trying to find outside investors?

25 A. Yes, they did.

1 Q. When did that happen?

2 A. That was in something like late June, early
3 July of 2001.

4 Q. Did you still have money available at that
5 time from what SAIC had already invested to continue
6 developing at least a test beta?

7 A. Yes, sir. They -- they did not pull back any
8 of the money. They let us keep what we had to continue
9 development.

10 Q. And did you do that?

11 A. Yes, sir, we did.

12 Q. How was that beta progressing in the late
13 summer of 2001?

14 A. I -- I was very pleased with it, and I told my
15 management that I thought they would be pleased with how
16 much progress we were making.

17 Q. I said that was in the late summer of 2001.

18 What effect did the events of September 11th,
19 2001, have on your team's ability to continue to work on
20 trying to make a business out of your invention?

21 A. Well, the -- the 9/11 event really changed a
22 lot of things. And for us, we always -- we had always
23 been working on national security problems, and -- and,
24 you know, that was kind of our -- felt like that was our
25 mission in life.

1 And -- and we started thinking about, you
2 know, what could we do to contribute to the -- you know,
3 in this new -- with this new threat.

4 Q. And what -- what projects did you devote your
5 time to?

6 A. I -- I ended up working on an unmanned aerial
7 vehicle mission planning system, provided some support
8 on the -- on the FBI counter-terrorism.

9 Q. Remind us what that FBI project was.

10 A. Yes, sir.

11 That was a -- it was an intelligence system to
12 try to collect information from a lot of different
13 sources, a lot of different databases, and try to
14 identify what people were doing and where the next
15 attacks might occur.

16 Q. And was that project for the FBI successful?

17 A. Yes, sir. I can't talk about the details, but
18 there were specific attacks that were stopped because of
19 that program, and there were lives saved.

20 Q. Let me show you a document, Dr. Short, that --
21 that I think you wrote. It's an e-mail, and it's
22 Defendant's Exhibit 3257.

23 Do you recognize that document?

24 It's in the book in front of you. You can't
25 see it very well on the screen.

1 A. Oh, it's hard to see on there.

2 Q. What is this e-mail?

3 A. I think that's the right one.

4 Oh, yes, sir, I recognize this.

5 Q. What is it?

6 A. This is an e-mail I sent in the November

7 timeframe in 2005 to Gif and to Vic Larson.

8 Q. And what were you talking about?

9 A. This is -- I was trying to understand what SIP
10 was all about. I had gotten a book and was reading on
11 SIP.

12 Q. Let me direct you to the second sentence of
13 your e-mail. You wrote to Mr. Munger and Mr. Larson --
14 that's Mr. Vic Larson, I guess, one of your
15 co-inventors.

16 And you said: Still reading through the book,
17 but I find myself losing the bubble on what
18 distinguishes us from SIPs, SIP-S.

19 What did you mean by that sentence?

20 A. Yeah, that's an expression I use.

21 I believe I was looking at SIPS, which is
22 secure SIP, in trying to figure out, okay, what
23 distinguishes our technology from -- point of view of
24 what features and capabilities do we provide that --
25 versus what SIPS provides. And at that point, I was

1 losing the bubble.

2 In other words, I was having trouble
3 distinguishing the significant differences in terms of
4 capabilities and features between the two.

5 Q. Were you referring to technical differences or
6 business differences?

7 A. I -- I think ultimately, at this point, I was
8 looking at potential market opportunities and, you know,
9 from the point of view of what could we offer the market
10 that was different.

11 Q. All right. Sometime around this time,
12 Dr. Short, did you learn that Mr. Munger, because of
13 some of the work he was doing, had begun to suspect that
14 Microsoft was infringing your patents?

15 A. Yes, sir.

16 Q. What was your reaction?

17 A. I was -- it was kind of mixed feelings. I
18 was -- I was surprised, but I was also gratified that a
19 company like Microsoft actually recognized the
20 significance of these ideas and these concepts.

21 And then I was also a little disheartened
22 that, you know, because there was an emerging
23 opportunity potentially for us to try to commercialize
24 this -- this technology again. And it appeared that
25 there were companies already using this technology. I

1 didn't see how we were going to be able to compete with
2 that.

3 Q. Did you think that Microsoft's use of your
4 invention would affect your abilities to introduce a
5 product to the user?

6 A. Oh, yes, sir.

7 Q. How?

8 A. Well, we were -- we were really small and, you
9 know, being able to -- to build and launch a product
10 that Microsoft was already in that space doing, I
11 thought would be extremely difficult and difficult to
12 get people to invest in because of the potential of
13 losing out to Microsoft.

14 Q. When did you learn that the company called
15 VirnetX had been formed?

16 A. That was probably in -- it was in 2005, I
17 believe.

18 Q. 2000 what?

19 A. 2005.

20 Q. Remember, speak up, please --

21 A. Yes, sir.

22 Q. -- so everybody can hear you.

23 Take a look at Defendant's Exhibit 3081.

24 What is this document?

25 A. This is -- this is a chain of e-mails.

1 Q. Is one of them an e-mail that you wrote to
2 Mr. Vic Larson at SAIC and Mr. Gif Munger in January of
3 2006?

4 A. Yes, sir.

5 Q. And you're discussing VirnetX in this e-mail,
6 correct?

7 A. Yes, sir.

8 Q. And one thing you wrote was that: As we
9 discussed on Monday, if we don't have an IP infringement
10 play, I don't see the play.

11 Do you remember writing that?

12 A. I do remember that, yes, sir.

13 Q. What did you mean by that?

14 A. Well, this goes back to what I -- what I just
15 said, that -- and what I meant by infringement play was,
16 if we can't defend our intellectual property, then we --
17 we can't keep people from competing with us using that
18 intellectual property.

19 And so if we can't prove infringement and
20 protect our property, I don't see how, from a business
21 point of view, we could survive.

22 Q. And when you -- when you say in your answer,
23 intellectual property that you needed to defend, you're
24 referring to what?

25 A. Well, I'm referring to these patents, yes,

1 sir.

2 Q. When did you join VirnetX?

3 A. That was in 2007. I think April of 2007.

4 Q. And you'd been with your company, SAIC, how
5 long at that time?

6 A. Over 10 years.

7 Q. And they had how many employees?

8 A. At that point, 60,000.

9 Q. 60,000?

10 A. Probably more. I'm not sure.

11 Q. And how many employees did VirnetX have?

12 A. 12.

13 Q. 12?

14 A. Yes, sir. Less than 12 at that point.

15 Q. At that point, less than 12?

16 A. Yes, sir.

17 Q. So, Dr. Short, after being at SAIC, a company
18 with 60,000 employees for 10 years, why did you decide
19 to leave there and join this company with less than 12
20 employees?

21 A. Before I came to SAIC, I had to convince
22 myself that we were really going to try to do something
23 real with this technology; in other words, we were going
24 to try to develop, license, make a real business out of
25 it.